

H2020 – BES – 5 – 2015

Research Innovation Action



Intelligent Portable ContROl SyStem



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626

D2.1 Requirements Analysis

Report Identifier:	D2.1		
Work-package, Task:	WP2	Status – Version:	1.00
Distribution Security:	CO	Deliverable Type:	R
Editor:	[REDACTED] (MMU) [REDACTED] (MMU)		
Contributors:	ALL		
Reviewers:	ITTI, JAS		
Quality Reviewer:	ED		
Keywords:			
Project website: www.icross-project.eu			

Copyright notice

© Copyright 2016-2019 by the iCROSS Consortium

This document contains information that is protected by copyright. All Rights Reserved. No part of this work covered by copyright hereon may be reproduced or used in any form or by any means without the permission of the copyright holders.

Table of Contents

ABBREVIATIONS.....	14
EXECUTIVE SUMMARY.....	22
1 INTRODUCTION.....	23
1.1 PURPOSE OF THIS DOCUMENT.....	23
1.2 STRUCTURE OF THE DOCUMENT.....	23
2 CONCEPTS OF BORDER MANAGEMENT	25
2.1 INTRODUCTION HISTORY OF BORDERS	25
2.2 BORDERS IN THE PRESENT.....	26
2.3 BORDER MANAGEMENT	27
2.4 INTEGRATED BORDER MANAGEMENT	27
2.5 BORDER POLICING	30
2.6 BASIC DEFINITIONS AND PRINCIPLES OF BORDER CONTROL.....	31
2.7 BORDER CHECKS IN HUNGARY	34
2.7.1 Detailed procedure of border checks in Hungary	35
2.7.2 Databases used during border check.....	38
2.7.3 Comparison of existing products features.....	39
2.8 REPUBLIC OF LATVIA	40
2.8.1 Border check procedure at the Terehova BCP.....	41
2.8.2 Border check procedure of the Zilupe BCP (railway)	45
2.8.3 Comparison of existing products features.....	51
2.9 TRAINOSE	53
2.9.1 The Thessaloniki – Eidomeni route.....	53
2.9.2 Procedures in passenger trains.....	54
2.9.3 Optional Procedures in freight trains	58
2.10 KEY POINT SUMMARY	63
3 STATE OF THE ART TECHNOLOGY REVIEW	64
3.1 EXISTING BORDER CONTROL PLATFORMS TECHNOLOGY REVIEW	64
3.1.1 APIS – Advanced Passenger Information System.....	64
3.1.2 PNR – Passenger Name Record.....	65
3.1.3 EES - Entry/Exit System.....	65
3.1.4 EURODAC - European Dactyloscopy	65
3.1.5 EUROSUR - European External Border Surveillance System.....	66

3.1.6	FADO and PRADO.....	66
3.1.7	Interpol FIND	66
3.1.8	SIS II – Schengen Information System II.....	67
3.1.9	VIS – Visa Information System.....	67
3.2	DOCUMENT AUTHENTICITY ANALYTICS TOOLS.....	68
3.2.1	Document authenticity verification device Regula 4205D	68
3.2.2	Coesys Document Verification.....	68
3.2.3	Keesing ID AuthentiScan PREMIUM.....	69
3.2.4	Identity Document and E-Passport Scanner (PRMc)	69
3.2.5	RealPass-V.....	69
3.2.6	DERMALOG VF1.....	69
3.2.7	OCR640e Desktop Full-page Document Imager.....	70
3.2.8	MBMS - Multi Border Management System	70
3.2.9	VISOTEC Expert 600	70
3.2.10	P1000	70
3.2.11	B5000	70
3.2.12	System and Method for Automatic Document Verification	71
3.2.13	Comparison	71
3.2.14	Summary.....	72
3.3	AUTOMATIC DECEPTION DETECTION SYSTEM (ADDS)	73
3.3.1	The Polygraph	73
3.3.2	Functional Magnetic Resonance Imaging (fMRI) detection	74
3.3.3	Electroencephalogram (EEG) detection	76
3.3.4	Voice Stress Analysis	76
3.3.5	Speech analysis	76
3.3.6	Facial Microexpressions.....	77
3.3.7	Silent Talker	79
3.3.8	Summary of State-of-the-Art Deception Detection Systems.....	80
3.3.9	Avatars and Supporting Technologies	81
3.3.10	Summary of Avatars and Supporting Technology applicable in iCROSS	84
3.4	BIOMETRICS.....	84
3.4.1	Fingerprint.....	85
3.4.2	Palm Vein readers.....	85

3.4.3	Voice Recognition	86
3.4.4	Facial Recognition.....	86
3.4.5	Iris Recognition.....	86
3.4.6	Retina Recognition	86
3.4.7	Comparative chart of biometric technologies	87
3.4.8	State of the Art in Facial Biometrics	87
3.5	HIDDEN HUMAN DETECTION TECHNOLOGY TOOLS.....	88
3.5.1	<i>Hidden Human Detection Technologies: Hidden Human Detection in Land Borders</i>	88
3.5.2	X-ray Systems	89
3.5.3	K9 Units and artificial sniffers - gas detectors	93
3.5.4	Non-ionizing Electromagnetic (EM) radiation – radars and microwave sensors.....	95
3.5.5	Geophones and their applications as heartbeat detectors.....	98
3.5.6	Metallic Containers Case: Acoustic (Sound) Sensors	100
3.5.7	Combination of Sensors.....	101
3.5.8	Summary – Conclusion and comparison of technologies.....	102
3.6	ANALYTICS (BCAT).....	104
3.6.1	State of the Art Analytical Approaches	104
3.6.2	Correlation Analysis.....	104
3.6.3	Pearson’s Correlation Coefficient.....	105
3.6.4	Summary.....	109
3.7	WIRELESS COMMUNICATION NETWORKS.....	109
3.7.1	Available Wireless Technologies for Radio Coverage and Connectivity.....	109
3.7.2	Network Dimensioning of the iCROSS Platform.....	113
3.7.3	Performance measures for the iCROSS network design.....	118
3.7.4	Conclusions.....	118
3.8	RELATED SURVEYS	119
3.9	RELATED RESEARCH PROJECTS	121
3.10	OVERALL CONCLUSION OF CURRENT STATE OF THE ART.....	126
4	REQUIREMENTS CAPTURE AND ANALYSIS.....	127
4.1	REQUIREMENTS CAPTURE METHODOLOGY	127
4.1.1	User Perspective.....	127
4.1.2	State-of-the-art Analysis	131
4.1.3	iCROSS system.....	131

4.2	CLASSIFICATION OF REQUIREMENTS	132
4.3	TRAVELLERS SURVEY ANALYSIS	134
4.3.1	Methodology for Traveller Closed Question Analysis.....	134
4.3.2	Results of Closed Question Analysis.....	135
4.3.3	Methodology for Traveller Open Question Analysis	145
4.3.4	Results for Open Question Analysis	145
4.3.5	Conclusions from Travellers Survey	149
4.4	STAKEHOLDER INTERVIEWS ANALYSIS	149
4.4.1	Analysis of Questions.....	149
4.4.2	Open Interview Questions.....	156
4.4.3	Summary.....	158
4.5	OUTLINE OF SCENARIOS FOR PILOT	159
4.5.1	“Pre-registration” general scenario:	161
4.5.2	“On border” crossing point check general scenario:	162
4.5.3	Description of specific situations:	163
4.6	CURRENT SITUATION AT CANDIDATE ICROSS PILOT SITES	165
4.6.1	Tompa-Kelebia BCP.....	165
4.6.2	Terehova road BCP	169
4.6.3	Zilupe railway BCP	172
4.6.4	Eidomeni – Gevgeli BCP.....	175
4.6.5	Summary.....	179
5	USER REQUIREMENTS.....	180
5.1	PRE-ARRIVAL PHASE	180
5.2	BACKGROUND CHECK PHASE	182
5.3	BORDER CHECK PHASE.....	183
5.4	GENERAL REQUIREMENTS	184
6	CONCLUSIONS	188
6.1	ACCOMPLISHMENTS	188
6.2	SUPPORT FOR FUTURE WORK	188
6.3	CONTRIBUTION TO ROADMAP	189
6.4	SUMMARY.....	189
7	REFERENCES.....	190
8	APPENDIX A TRAVELLERS QUESTIONNAIRE	202

8.1	ENGLISH TEMPLATE.....	202
8.2	HUNGARIAN VERSION	205
8.3	CHINESE VERSION	210
8.4	ARABIC VERSION	215
8.5	FRENCH VERSION	222
8.6	GERMAN VERSION	227
8.7	RUSSIAN VERSION	232
8.8	SPANISH VERSION	237
8.9	LATIN VERSION.....	242
8.10	GREEK VERSION.....	246
8.11	CROATIAN VERSION	251
8.12	TURKISH VERSION	255
9	APPENDIX B LEAFLET READABILITY METHODOLOGY	260
10	APPENDIX C TRAVELLERS LEAFLET	262
10.1	ENGLISH VERSION	262
10.2	HUNGARIAN VERSION	263
10.3	SERBIAN VERSION	264
10.4	GERMAN VERSION	265
10.5	ARABIC VERSION	266
10.6	SPANISH VERSION	267
10.7	RUSSIAN VERSION	268
10.8	GREEK VERSION.....	269
10.9	LATIN VERSION.....	270
10.10	CHINESE VERSION	271
10.11	FRENCH VERSION	272
10.12	TURKISH VERSION	273
11	APPENDIX D ICROSS LETTER OF INFORMED CONSENT AND INFORMATION SHEET	274
12	APPENDIX E BORDER GUARD INTERVIEW PROTOCOL.....	277
12.1	ENGLISH VERSION	277
13	APPENDIX F BORDER GUARD INTERVIEW LIST OF QUERIES.....	279
14	APPENDIX G RESULTS FROM TRAVELERS QUESTIONNAIRE	282
15	APPENDIX H STATISTICAL ANALYSIS OF THE RESULTS FROM THE BORDER GUARD / MANAGERS INTERVIEWS.....	305

List of Tables

TABLE 1 BORDER TYPES AND ASSOCIATED BORDER CHECKS.....	32
TABLE 2 COMPARISON EXISTING PRODUCE FEATURES AGAINST ICROSS.....	39
TABLE 3 DESCRIPTION OF DATABASES USED BY STATE BORDER GAURD OF LATVIA.....	48
TABLE 4 COMPARISON OF EXISTING PRODUCT FEATURES AGAINST ICROSS INNOVATIONS.....	52
TABLE 5 COMPARISON OF EXISTING PRODUCTS FEATURES AGAINST ICROSS INNOVATIONS.....	71
TABLE 6 IMPORTANT FEATURES OF LIE DETECTION SYSTEMS FOR POTENTIAL APPLICATION IN ICROSS.....	80
TABLE 7 IMPORTANT FEATURES OF AVATARS FOR POTENTIAL APPLICATIONS IN ICROSS	83
TABLE 8 COMPARATIVE OVERVIEW OF BIOMETRIC TECHNOLOGIES.....	87
TABLE 9 TABLE DESCRIPTION	87
TABLE 10 COMPARATIVE OVERVIEW OF TECHNOLOGIES FOR HUMAN DETECTION.....	102
TABLE 11 802.11X STANDARDS	110
TABLE 12 MICROWAVE LINKS AND APPLICATIONS	110
TABLE 13 EVOLUTION OF CELLULAR NETWORKS.....	111
TABLE 14 TECHNICAL DETAILS OF DVB-S-STANDARDS.....	113
TABLE 15 ANTENNA DIAMETERS AND RESPECTIVE EIRP VALUES FOR SUPPORTING AREA OF THE SATELLITE LINK	117
TABLE 16 CONNECTION OF PERFORMANCE MEASURES WITH TCP/IP PROTOCOLS STACK.....	118
TABLE 17 COMPARISON AND INNOVATION AND FOCUS ON EXISTING PROJECTS	125
TABLE 18 REQUIREMENTS SYNTAX	133
TABLE 19 STRUCTURE OF SYSTEM REQUIREMENT TABLES	133
TABLE 20 MoSCoW PRIORITIZATION TECHNIQUE	134
TABLE 21 BREAKDOWN OF NAMED LOCATIONS WITH NEGATIVE SENTIMENTS.....	146
TABLE 22 CROSS TAB AGE * JOB EXPERIENCE.....	153
TABLE 23 CHI SQUARE TESTS FOR AGE * JOB EXPERIENCE	153
TABLE 24 CROSS TAB AGE * JOB EXPERIENCE IN CURRENT POSITION	153
TABLE 25 CHI-SQUARE TESTS FOR AGE * JOB EXPERIENCE IN CURRENT POSITION	154
TABLE 26 CROSS TAB NATIONALITY * AVERAGE WAIT TIME FOR THIRD COUNTRY NATIONALS AT YOUR BORDER GATE (ABSOLUTE WAIT TIME).....	154
TABLE 27 CHI-SQUARE TESTS (ABSOLUTE WAIT TIME)	154

TABLE 28 PROFESSIONAL STATUS * WHAT IS YEARLY AVERAGE PASSENGER RATE OF THIRD COUNTRY NATIONALS AT THE BORDER GATE?.....	154
TABLE 29 CHI-SQUARE TESTS PROFESSIONAL STATUS * YEARLY AVERAGE PASSENGER RATE OF THIRD COUNTRY NATIONALS AT THE BORDER GATE.....	155
TABLE 30 BORDER GATE TYPE * AVERAGE WAIT TIME FOR THIRD COUNTRY NATIONALS (ABSOLUTE WAIT TIME)	155
TABLE 31 CHI-SQUARE TESTS BORDER GATE VERSES ABSOLUTE WAIT TIME	156
TABLE 32 ICROSS SYSTEM INVOLVED IN “PRE-REGISTRATION” GENERAL SCENARIO.....	161
TABLE 33 ICROSS SYSTEM INVOLVED IN “ON BORDER” CROSSING POINT	163
TABLE 34 ICROSS SYSTEM INVOLVED IN SPECIFIC SCENARIOS.....	164
TABLE 35 VEHICLE TRAFFIC.....	166
TABLE 36 PASSENGER TRAFFIC.....	167
TABLE 37 MISCARRIAGES	168
TABLE 38 PASSENGER FLOW AT TEREHOVA BCP IN 10-MONTH PERIOD (2015-2016).....	170
TABLE 39 FLOW OF VEHICLES AT TEREHOVA BCP IN A 10-MONTH PERIOD (2015-2016)	171
TABLE 40 VIOLATION STATISTICS DETECTED AT TEREHOVA BCP	171
TABLE 41 ZILUPE RAILWAY BCP STATISTICS (1ST JANUARY TO 31ST OCTOBER).....	173
TABLE 42 FLOW OF TRAINS AT ZILUPE RAILWAY BCP IN THE 10-MONTH PERIOD (2015 - 2016)	174
TABLE 43 VIOLATIONS DETECTED ON THE TRAIN AT ZILUPE	174
TABLE 44 PASSENGER / IMMIGRANT STATISTICS ON THE THESS-EIDOMENI ROUTE.....	176

List of Figures

FIGURE 1 OLD BORDER TYPES	25
FIGURE 2 CONTEMPORARY BORDERS.....	26
FIGURE 3 BORDER MANAGEMENT MODELS	27
FIGURE 4 EUROPEAN SECURITY MODEL	28
FIGURE 5 THE FOUR TIER ACCESS CONTROL MODEL.....	29
FIGURE 6 CURRENT SCHENGEN AND EU OVERLAP (2016).....	30
FIGURE 7 EU INTERGRATED BORDER MANAGEMENT CONCEPT	31
FIGURE 8 BORDER POLICING FLOW	31
FIGURE 9 BORDER CHECKS.....	33
FIGURE 10 BORDER CROSSING POINT IN HUNGARY	35
FIGURE 11 TOMPA BORDER CROSSING	37
FIGURE 12- SIS II GUI (DR VASS ZSOLT)	39
FIGURE 13 BORDER CROSSING AT TEREHOVA	42
FIGURE 14 FIRST LINE BORDER CHECK PROCESS.....	43
FIGURE 15 SECOND LINE BORDER CHECK PROCESS	44
FIGURE 16 DOCUMENT AUTHENTICITY PROBLEM.....	44
FIGURE 17 SECOND LINE PROCESS WHEN A DATABASE 'HIT' OCCURS	45
FIGURE 18 RAILWAY BORDER CROSSING POINTS.....	46
FIGURE 19 FIRST LINE BORDER CHECK PROCESS.....	46
FIGURE 20 LOCAL MAP OF RAILWAY NETWORK	53
FIGURE 21 THESSALONIK PASSENGER STATION	54
FIGURE 22 TYPICAL HANDWRITTEN TICKETS	55
FIGURE 23 TICKET WRAPPER.....	55
FIGURE 24 PASSENGER UNIFORM TICKET.....	56
FIGURE 25 TICKET FOR CAR TRANSFER.....	56
FIGURE 26 TYPICAL BMZ PASSENGER WAGON	57
FIGURE 27 DRAWINGS OF BMZ WAGON	57
FIGURE 28 INSIDE OF A WAGON	58
FIGURE 29 BULK WAGON	59

FIGURE 30 COVERED WAGON	59
FIGURE 31 TANK WAGON.....	60
FIGURE 32 CONTAINER WAGON.....	60
FIGURE 33 RAILWAY MAP OF NORTH GREECE.....	61
FIGURE 34 CIM DOCUMENT.....	62
FIGURE 35 CONTAINER SECURITY SEAL.....	62
FIGURE 36 THE POLYGRAPH.....	74
FIGURE 37 PHILIPS MRI SCANNER	75
FIGURE 38 FMRI SCANNER.....	75
FIGURE 39 EEG ELECTRODE PLACEMENT.....	75
FIGURE 40 ANALYSIS OF TEXT	77
FIGURE 41 UNIVERSAL FACIAL EXPRESSIONS OF EMOTION.....	78
FIGURE 42 SILENT TALKER ARCHITECTURE	79
FIGURE 43 HIDDEN PERSONS IN CARS (REAL CASES, PHOTOS PROVIDED BY PARTNER HNP)	89
FIGURE 44 LEIDOS VACIS® IP6500 CARGO INSPECTION SYSTEM (OFFICIAL VIDEO).....	91
FIGURE 45 RAPISCAN SERIES OF PRODUCTS	91
FIGURE 46 SMITHS DETECTION SERIES OF PRODUCTS	92
FIGURE 47 POLICE DOG IN WISCONSIN (SOURCE: WIKIPEDIA)	93
FIGURE 48 ION SENSOR SM-24 ROTATING COIL GEOPHONE.....	98
FIGURE 49 AVIAN HEARTBEAT DETECTOR BY ONEX SA - SOURCE: GEOVOX.COM AND ONEX SA.....	99
FIGURE 50 RDC COMPUTATION.....	105
FIGURE 51. K-MEANS CLUSTERING WITH K=4.....	107
FIGURE 52 HIERARCHICAL CLUSTERING REPRESENTATION WITH A HEATMAP.	108
FIGURE 53 THE DECISION BOUNDARY IS $Y=0$ WHEREAS THE MARGIN IS THE PERPENDICULAR DISTANCE BETWEEN THE DECISION BOUNDARY AND THE CLOSEST DATA POINTS OF THE TWO CLASSES	109
FIGURE 54 ARCHITECTURE OF DVB-S/S2 AND DVB-RCS NETWORKSARCHITECTURE OF DVB-S/S2 AND DVB- RCS NETWORKS	112
FIGURE 55 FORWARD/REVERSE CONNECTIONS FOR THE APPLICATION SERVICES.....	113
FIGURE 56 NETWORK PROTOCOLS STACK.....	114
FIGURE 57 DEPLOYMENT SOLUTIONS FOR THE ICROSS NETWORK	116
FIGURE 58 SUPPORTING AREA OF THE SATELLITE LINK	116

FIGURE 59 STATE TRANSITION DIAGRAM OF THE FINITE SOURCE MODEL	117
FIGURE 60 REQUIREMENTS METHODOLOGY OVERVIEW	127
FIGURE 61 RELATIONSHIP BETWEEN D2.1 AND D2.2.....	132
FIGURE 62 iCROSS USER REQUIREMENTS AND DESCRIPTION OF SERVICES.....	132
FIGURE 63 QUESTION 1 ANALYSIS - WHAT IS YOUR PRIME REASON FOR TRAVELLING ACROSS EU SCHENGEN BORDERS?	135
FIGURE 64 QUESTION 2 ANALYSIS - HOW OFTEN DO YOU TRAVEL?	136
FIGURE 65 QUESTION 3 ANALYSIS - WHAT MEANS OF TRANSPORT DO YOU PREFER?	136
FIGURE 66 QUESTION 4 ANALYSIS - WHAT MOBILE DEVICE DO YOU USE WHEN TRAVELLING?	137
FIGURE 67 QUESTION 6 ANALYSIS - HOW USEFUL IS REAL TIME INFORMATION ABOUT BORDERS TRAFFIC BEFORE ARRIVAL?	138
FIGURE 68 QUESTION 8 ANALYSIS - WHAT SOCIAL MEDIA DO YOU USE?	139
FIGURE 69 QUESTION 9 ANALYSIS - WHEN IS THE MOST IMPORTANT TIME THAT YOU ACCESS INFORMATION IN ADVANCE OF YOUR TRAVELS?	140
FIGURE 70 QUESTION 10 ANALYSIS - WHERE DO YOU ACCESS INFORMATION RELEVANT TO YOUR TRAVEL?.....	140
FIGURE 71 QUESTION 11 ANALYSIS - HAVE YOU EVER SUPPLIED ADVANCED PASSENGER INFORMATION?.....	141
FIGURE 72 QUESTION 13 ANALYSIS - RESPONSES.....	141
FIGURE 73 QUESTION 13 - ANALYSIS - TRAVEL DESTINATIONS.....	142
FIGURE 74 BREAKDOWN OF PRE-TRAVEL INFORMATION SYSTEMS USED BY TRAVELLERS.....	142
FIGURE 75 QUESTION 14 ANALYSIS - HOW LONG WOULD YOU EXPECT TO SPEND ON PRE-TRAVEL REGISTRATION?	143
FIGURE 76 QUESTION 15 ANALYSIS - QUESTIONS TRAVELLERS ARE PREPARED TO ANSWER AT PRE-REGISTRATION.	143
FIGURE 77 QUESTION 16 ANALYSIS - WHERE WAS YOUR MOST RECENT BORDER CROSSING?.....	144
FIGURE 78 QUESTION 17 ANALYSIS - TIME TAKEN TO CROSS THE BORDER.	144
FIGURE 79 QUESTION 19 ANALYSIS - SENTIMENT OF WORST BORDER CROSSING.....	145
FIGURE 80 QUESTION 19 ANALYSIS - WORD CLOUD	146
FIGURE 81 QUESTION 20 WORD CLOUD	148
FIGURE 82 JOB EXPERIENCE OF SURVEY PARTICIPANTS	150
FIGURE 83 JOB EXPERIENCE AT CURRENT POSITION	150
FIGURE 84 YEARLY AVERAGE PASSENGER RATE OF THIRD COUNTRY NATIONALS AT THE BORDER GATE.....	151

FIGURE 85 AVERAGE WAITING TIME FOR THIRD COUNTRY NATIONALS AT THE BORDER GATE, FROM THE ARRIVAL AT THE GATE TO LEAVING THE GATE	152
FIGURE 86 AVERAGE CONTROL TIME FOR THIRD COUNTRY NATIONALS AT THE BORDER GATE, FROM BEGINNING HIS/HER CROSSING FOR ADMISSION / EXIT DECISION.....	152
FIGURE 87 PROPORTION (ESTIMATED PERCENTAGE) OF VEHICLES SEARCHED DURING THE BORDER CHECK)	152
FIGURE 88 ICROSS WORKFLOW.....	160
FIGURE 89 TOMPA-KELEBIA BCP.....	166
FIGURE 90 LOCATION OF TOMPA-KELEBIA BCP.....	166
FIGURE 91 BORDER CROSSING POINT IMAGES	168
FIGURE 92 TEREHOVA BCP ENTRY TO LATVIA	170
FIGURE 93 BORDER CHECK ON THE TRAIN	172
FIGURE 94 REGULA 8333.111 MOBILE DEVICE USED FOR PERFORMING BORDER CHECKS ON THE TRAIN	173
FIGURE 95 RESULT OF DETECTION OF SMUGGLED GOODS (CIGARETTES).....	175
FIGURE 96 FASTEST PATH TO EU ZONE THROUGH EIDOMENI BORDERS	175
FIGURE 97 LOCATION OF ATHENS TERMINAL.....	176
FIGURE 98 CONTAINERS PARKED INSIDE ATHENS TERMINAL	177
FIGURE 99 FREIGHT TERMINAL OF THESSALONIKI	177
FIGURE 100 THESSALONIKI TERMINAL	178
FIGURE 101 EIDOMENI BORDER CROSSING POINT.....	178

Abbreviations

1D	One dimensional
2D	Two dimensional
24/7 Interpol (I-24/7)	a secure global police network that enables investigators to access INTERPOL's range of criminal databases
4G	Fourth-generation wireless telephone technology
ABC	Automated Border Control
ACM	Adaptive Coding & Modulation
ADDS	Automatic Deception Detection System
AFIS	Automated Fingerprint and palmprint Identification System
ALO	Airline Liaison Officer
ANN	Artificial Neural Network
API	Advanced Passenger Information
APIS	Advanced Passenger Information System
AuthentiScan	Authentication scanner for passports, ID cards, driving licenses, visas and residence permits
AVIAN	Advanced Vehicle Interrogation And Notification
AWF	Analysis Work File (Europol AWF)
BC	wagon 2nd class couchette
BC, BCE	number of years before starting point (0) of common European dating system
BCAT	Border Control Analytics Tool
BCP	Border Crossing Point
BES-05-2015	Border crossing points topic 1: Novel mobility concepts for land border security 2015
BIOSEC	A biometric personal identification system
BIPS	Biometric Passports Information System

BMZ	Bryansk Machine-building Plant (railway wagon)
BTT	Hungarian Database: persons expelled from Hungary
BÜ	Hungarian Database: register of crimes and offences
CIM	Convention Internationale concernant le transport des Marchandises par chemin de fer (An internationally standardized freight document issued in rail transport)
CIV	Convention Internationale pour le transport des Voyageurs
COTIF1999	Convention concerning. International Carriage by Rail
CSDD	Latvian Database: Data base of the Road Traffic and Security Directorate
CSS	Capital Services System
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
CVIS	Latvian Database: Central Visa Information System
CW	Continuous Wave
DAAT	Document Authenticity Analytics Tool
DCF	Distributed Coordination Function
DDam	three-axle wagon for transport of cars
DERMLOG VF1	a scanner able to capture fingerprint and passport images on the same scanning surface
DMU	Diesel Multiple Unit
Dn.n	Deliverable (report identifier)
DVB-RCS	Digital Video Broadcasting – Return Channel via Satellite (or over System)
DVB-S	Digital Video Broadcasting – Satellite – First Generation
DVB-S2	Digital Video Broadcasting – Satellite – Second Generation
EC	European Commission
EEG	ElectroEncephaloGram
EES	Entry-Exit System EES
e-Gate	automatic crossing gate

Electromagnetic	Electromagnetic
EMU	Electric Multiple Unit
ENS	Entry Summary Declaration
Entas UVEC	A document scanner
EU	European Union
EUR-Lex	A website providing access to European Union Law
EURODAC	European Dactyloscopy (applied to verify the fingerprints of asylum seekers as well as illegal migrants)
Eurojust	An agency of the European Union dealing with judicial co-operation in criminal matters.
EUROPOL	European Police Office
EUROSUR	European External Border Surveillance System
EXS	Exit Summary Declaration
FADO	False and Authentic Documents Online
FAQ	Frequently Asked Questions
FAR	False Acceptance Rate
FIND	Fixed INTERPOL Network Database
fMRI	functional Magnetic Resonance Imaging
FMT	Face Matching Tool
FOSS	Frontex One-Stop-Shop
FRONTEX	Frontières extérieures for "external borders"
FRR	False Rejection Rate
FYROM	former Yugoslav Republic of Macedonia
GHz	GigaHerz - one thousand million (10 ⁹) cycles per second
GUI	Graphical User Interface
HERMON	Hungarian Database: national wanted database

HERR	Határ Ellenőrző és Regisztrációs Rendszer (Border Check and Registration System)
HERRWEB	A module used to search the Hungarian national entry-exit database
HHD	Hidden Human Detection
HIDRA	Hungarian Immigration Control and Enforcement System
Horus 1018	A document scanner
IÁIAR	Register of expelled foreigners and prohibition of entry
IBM	Integrated Border Management
ICAO	International Civil Aviation Organization
iCROSS	Intelligent Portable ContROl SyStem
ICT	Information and Communication Technology
ID	Identification (or Identity)
IEEE	Institute of Electrical and Electronic Engineers
iFADO	intranet False and Authentic Documents Online
IIIS	Latvian Database: Integrated Information System of the Ministry of Internal Affairs
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
IPL	Hungarian Database: register of Hungarian nationals and residents
IR	Infra-Red
ISO	International Standards Organisation
IT	Information Technology
ITTI	ITTI SP ZOO, iCROSS partner, SME
JÁRMŰ	Hungarian Database: vehicle, vehicle license and insurance register
JÁROK	Hungarian Database: vehicle, vehicle license and insurance register
JAS	JAS technologie sp. z o.o., iCROSS partner, SME
LED	Light Emitting Diode

LEICA MS5	High-performance stereomicroscope
LTE	Long Term Evolution
M1 - Mn	Month of project
M2M	Mobile to Mobile (also Machine-to-Machine)
MAC	Medium Access Control
MBMS	Multi Border Management System
MIMO	multiple-input and multiple-output
MIND	Mobile INTERPOL Network Database
MMU	Manchester Metropolitan University
mm_wave	millimeter-wave frequencies
MRI	Magnetic Resonance Imaging
MRZ	Machine Readable Zone
NDR	Latvian Database: 1.2. Invalid Document Register
NEKOR	genuine document security marks and forged documents register
NVB	Non-Verbal Behaviour
NVIS	Latvian Database: National Visa Information System
OCR	Optical Character Recognition
OCR640e	full-page multi-illumination ePassport reader
OSE	Hellenic Railways Organization (also Greek passenger rail car)
PAPILLON DS-30N	Fingerprint Scanning Device
PC	Principal Component
PCC SEE	Police Cooperation Convention for Southeast Europe Secretariat
PDP	The Population register software "Individuals Data Browser"
PIU	Passenger Information Unit
PMMW	Passive mm-wave imaging

PNR	Passenger Name Record
PRADO	Public Register of Travel and Identity Documents Online
PREMIUM	an automated solution for extensive ID document authentication
PRMc	a (full-page) multi-purpose scanner
QR	Quick Response (code)
R	Deliverable type
RBAT	Risk Based Assessment Tool
RCS	Radar Cross Section
RealPass	Full Page Optical & RFID Passport Reader
Regula 1025.01	authenticity verification and advanced examination of passports, ID cards and other travel documents
Regula 4205	Document authenticity verification device
Regula 7024.111	Document scanner
Regula T8333	a piece of mobile document examination equipment
REIS - 2002	Latvian border crossing control system / a register of border crossing persons and vehicles
RF	Radio Frequency
RFID	Radio Frequency Identification
RR	Reflection Removal
RTP	(Voluntary) Registered Traveller Program
SA	Schengen Accession
Sagem MS0100	Sagem Morphosmart Fingerprint and Identification Scanner
SBG	State Border Guard of the Republic of Latvia
SDK	software development kit
SIRENE	Supplementary Information Request at the National Entry
SIS	Schengen Information System

SIS II	Schengen Information System v2
SMIC	Spontaneous Micro-expression Database
SOP	Standard Operational Procedures
SPS	SharePoint Portal Services (Microsoft a secure place to store, organize, share, and access information)
ST	Silent Talker
SZABS	Hungarian Database: register of crimes and offences
SZIG	Hungarian Database: passport and ID database of Hungarian nationals and residents
SZL	Hungarian Database: register of Hungarian nationals and residents
TCN	Third Country National
TRAINOSE	TrainOSE S.A. is a railway company in Greece which currently operates all passenger and freight trains on OSE lines
UIC 505-1	(specification of) a railway gauge
UK	United Kingdom of Great Britain and Northern Ireland
UTL	Hungarian Database: passport and ID database of Hungarian nationals and residents
UTTL-K	Hungarian Database: persons restricted from travel
UV	Ultraviolet
UWB	Ultra-Wide Band
TWIS	Through the wall imaging system
UTTL-K	Hungarian Database: persons restricted from travel
UV	Ultraviolet
VIN	Vehicle Identification Number
VIS	Visa Information System
VISA 2	Visa Information System 2 nd generation
VIZ	Visual Inspection Zone

VMIS IĀIAR	Latvian Database: Expelled aliens and prohibition of entry of the Integrated Migration Information System (one or two databases?)
VSC	Video Spectral Comparator
VSC4CX	VIDEO SPECTRAL COMPARATOR the compact workstation for the examination of questioned documents
VSC-6000/HS	video spectral comparator (Document examiner)
WLB	sleeping car 2nc class
WPn.n	Work Package
WP	Work Package
WWI	World War 1
ZF CARGO	the major railway operator of FYROM

Executive Summary

The purpose of this report is to analyse the requirements of the iCROSS components. A comprehensive understanding of a range of issues is required for the successful production of individual iCROSS deliverables and their coherent inter-working to discharge all of their requirements under the EC grant contract. This is achieved through a number of stages.

The first stage is a review of the underlying concepts of border management, providing an understanding of operational issues from the end users in their geographical context. The second stage reviews the state of the art of research and development for the various technological components of iCROSS, within a perspective of existing practice. Each of these sections contains a summary table of functions or relevance to iCROSS, whose form is appropriate to the maturity of the technology. The third stage develops the stakeholders' requirements, through interviews and questionnaires. This information is codified into use case scenarios, which will inform developmental experiments and evaluation of iCROSS.

D2.1 is a communicative tool supporting iCROSS' meeting the EC Grant Contract requirements by ensuring comprehension and coverage of the design, production and evaluation requirements of the iCROSS border crossing solution by the consortium partners.

1 Introduction

1.1 Purpose of this Document

This report describes Task 2.1, the process of capturing the requirements for iCROSS, which satisfies the first objective and deliverable in WP2.

The overall objectives of WP2 are to:

- To analyse the end-user requirements and to assess user functional and technical needs.
- To identify the processes, technologies, challenges and their shortcomings through participatory research.
- To develop the iCROSS reference architecture and component / module specifications.
- To conduct a thorough legislation review, both in EU and national level, to ensure iCROSS's legal compliance and to address privacy issues related to border control pilot scenarios i.e. agreements and informed consent.

The analyses performed in this task will ensure that the iCROSS product will address the challenges set out in our response to topic 1: Novel mobility concepts for land border security, in the BES-05-2015 Border crossing points call. Therefore, the Requirements Analysis consists of structured and integrated sections to ensure that the design objectives of iCROSS are met. This document will act as a point of reference for iCROSS partners on resolution of design requirement issues.

The elicitation of requirements is divided into 4 distinct phases:

- Contextual analysis through the collation of concepts of border management
- A review of the state of the art of technologies which are (or could be) used in border management
- Capture of users' opinions and experience of the border crossing activity
- Codification of user requirements

Thus, D2.1 will support the quality management plan (D8.1) by early detection and prevention of errors caused by misinterpretation of requirements and responsibilities for their fulfilment.

1.2 Structure of the Document

The structure of this document is as follows:

- Section 2 comprises a description and analysis of concepts of border management. This includes historical context, current practice and a European perspective on Integrated Border Management. It then reviews individual practices at the Border Control Points of end users: Hungarian National Police, the Latvian Border Guard and TRAINOSE (Greek Rail Border Crossing Points).
- Section 3 begins with a review of the state of the art of the technology of current border control platforms and that used by the iCROSS end users in particular. It proceeds with reviews of the technologies proposed for iCROSS, including document analysis tools, lie detection and avatars (for ADDS), Biometric technologies for identification, technologies for the detection of hidden humans / contraband, analytics technologies for data mining and optimising the performance of iCROSS (for BCAT), and wireless communications networks

to integrate travellers, iCROSS components and border guards in the field. Finally, it reviews relates surveys and recent research in the field.

- Section 4 firstly outlines the methodology adopted for requirements capture and analysis to complement the state of the art review with the user perspective. This elicits both the functional and non-functional requirements. It explains how the perspective is informed by questionnaires and a site survey with a practical workshop [REDACTED]. The questionnaires use categorical answers, Likert scale answers and projective questions to verify or move beyond the current knowledge of consortium members. It contains a delivery strategy to optimise useful responses and methods to enhance the speed of analysis - and so provide timely information to shape the iCROSS approach. It concludes with a set of scenarios to inform experimental design and evaluation and information of candidate pilot sites.
- Section 5 describes the general user requirements which have been extracted from the traveller's survey results, Border Guard survey results, Border Guard Officers and Managers interview results and the expertise of the participating end users. The extracted general user requirements for the system, will be the input for the deliverable D2.2 – Reference Architecture and Components specifications.

2 Concepts of Border Management

2.1 Introduction History of Borders

A border is like skin. It has two ambivalent purposes: to separate and to connect. It separates the territory as an area controlled by a given group of people from areas controlled by other groups or by no one. Such a behaviour may arise for reasons of protection, securing resources etc. and may spark aggression against trespassers (Stout, 1975). On the other hand, it keeps members of the group together, enhances task distribution (sentinels arise) and serves as identity basis for the socio-geographical group (Tatalovic, 2010). In the early period of human civilization, tribes were living in the wildernesses and the only place where they could feel themselves relatively safe, was within their borders, serving as frontiers. Becoming an outcast or being expelled even for a short time was almost equal to the death sentence. For example, before 130 BC, to spend one night without weapons, armor and fire outside of the camp was one of the most serious punishments in a Roman legion, second only to decimation (Goldberg, 2016). Trespassers were automatically treated as enemies, chased down, killed (sacrificed) and in several cases, eaten (Erman, Grapow, & Erichsen, 1950). Later when ancient trade was invented, hospitality emerged. First, in form of sacred rituals protecting the guest (O'Gorman, 2010) (Sabloff, 1975).

As technology evolved and humanity took control over most regions, borders usually became a place for trade and of course, place of taxation. Before the birth of national states, borders were everywhere, between cities, tenures and so on (Tilly & Ardant, 1975). Instead of passports, travellers used tokens of friendship of someone protecting them in the foreign land (proxinoi) or "laissez-passer" type papers. The first of such papers found is from 450 BC ("Letter to the lords across the river [in Judea]" by Artaxarxes, ruler of Persia) (Blenkinsopp, 1987). Also acting for the purpose of protection, some border sections were reinforced and used as frontiers, like the Roman limes (guarded by military troops: limitanei or ripenses) or the Chinese Great Wall (Treadgold & Treadgold, 1998). Reverting into the "original" or "first" purpose of the borders, to keep anything else out. None of the walls built were able to protect the territory permanently, both the Roman limes and the Great Wall were breached, as more recently was the Iron Curtain and the Wall of Berlin. Territory cannot be protected solely at the borderline. Protection of Territory is a complex activity called Integrated Border Management, performed by many actors inland, at the border and in foreign territory



Figure 1 Old border types

(Varga, 2015). Nowadays, as we live in the age of nation-states, the key actors are the sovereign entities of nation states and for them, territory is an essential element of existence (Habermas & Ciaran, 1998).

2.2 Borders in the present



Figure 2 Contemporary borders

Germany, as if his/her plane - for example - is registered in Germany (e.g. Lufthansa plane), legally, the traveller can be located in German territory from engine power set for departure until opening cabin doors at destination

(Bonassies, 1969). On the other hand, land borders are crossed at border gates, at the (or very near to) the demarcation line and in most of cases, passengers are checked while sitting in their vehicles. This is the border check, which is only one, but the most important part of the Integrated Border Management and its Four-Tier Access Model (Lanfermann, 2014).

Borders are directly related to the existence of a nation-state. As by the definition of “nation-state”, demarcated territory and exclusive power over the territory are two key pillars in sovereignty (permanent population, one government and the capacity to enter into relations with other sovereign states are the other pillars) (Péter, 1997) (N. Shaw, 2003). If the borders are not able to fulfill either of their purposes, to separate (defined territory and exclusive power over the territory) and to connect (help to keep together permanent population and be allowed to enter into relations with other sovereign states), the existence of the nation-state itself becomes endangered. The same danger arises when the border is shifted radically to just one of the two purposes: open borders which create security deficit, closed borders which create illegal migration and at the end, physical aggression (Mária, 2007). There are three types of borders, delimited by international treaties and demarcated by border signs: **open borders**, which can be crossed at almost any time and place (e.g. from Germany to Austria), **controlled borders** (e.g. from Hungary to Romania), where a traveller can cross at border gates but otherwise, it is prohibited, and **closed borders** which are more like frontiers (e.g. from North Korea to South Korea). By type, borders can be air borders, sea borders and land borders (including borders across inland water) (Sallai, 2004). The procedure of protecting the borders against unauthorized border crossing is called border surveillance in most countries. Border surveillance is a considerable challenge, especially at sea borders, but it is out of the scope of this project and only covered as much as necessary. In case of sea and air borders, the actual border crossing and the border control is separated in time and space, as those vessels are under the “loi du pavillon”: the traveller can cross the Hungarian-Slovakian border when he/she is sitting on a plane flying from Bratislava to Budapest, but will only be controlled after the plane lands in Budapest. Additionally, it may be that meanwhile the passenger will have a seat in

2.3 Border Management

Border management means regulating, controlling and facilitating the cross-border flow of persons, goods and services, through border policing, immigration control, asylum, customs check, nature protection, sanitary control and cross-border crime prevention measures. The first documented border management system operated in 1287 BC at the Egyptian-Nubian border, established by I. Seth, with base in the Fortress of Semna, consisting of stationary and mobile Medjay, units enforcing border policy (Erman, Grapow, & Erichsen, 1950). Border management is split between military border protection and administrative borders. There are different border management models around the world (Figure 3), built around same basic approach but following different principles (Varga, 2015). This basic approach is cooperation and coordination between stakeholders.



Figure 3 Border Management Models

For this project, based on the text of the call, the focus will be on EU's Integrated Border Management, the connecting European Security Model and the border policy of individual Member States (MS) (on the example of Hungary). However, for future exploitation purposes of the solution, other border management solutions will be taken into account, to maintain compatibility with potential future non-EU customers.

2.4 Integrated Border Management

The Integrated Border Management (IBM) approach aims to create the balance between facilitation of the flow of persons and goods across borders and providing security measures in order to achieve sustainable border management. Originally developed by the Schengen MSs, Integrated Border Management was integrated into the EU acquis with the Treaty of Amsterdam, 1999 (Moravcsik & Nicolaïdis, 1999). Later it was implemented by many other countries especially along main migration routes. It recognizes that maintaining border security and controlling immigration is a complex challenge and is not solely the task of border control agencies.

It is part of the European Security Model established (Figure 4) by the Stockholm Programme and described by European Security Strategy renewed in every five years, starting with 2003 (Varga, 2015).

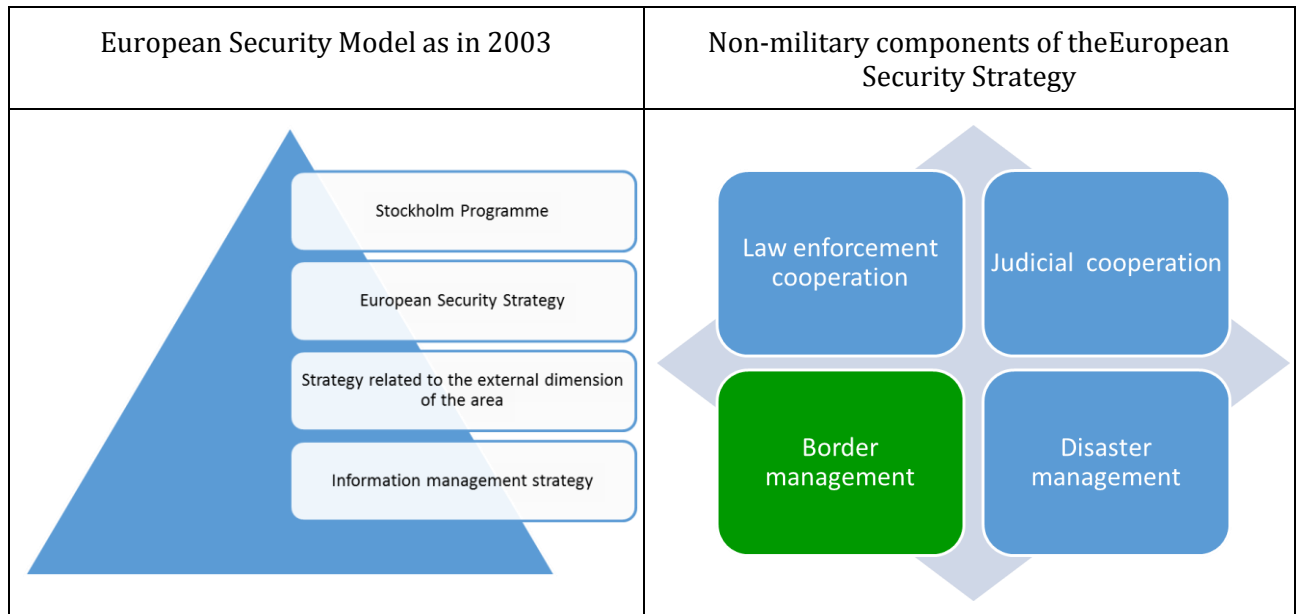


Figure 4 European Security Model

IBM is a system operated by various actors for a common goal. Cooperation is the key to achieve it. Within IBM, the three pillars of the cooperation are:

- Intra-service cooperation
- Interagency cooperation
- International cooperation

Cooperation has to be facilitated through:

- legal and regulatory framework
- Institutional framework
- Procedures (Standard Operational Procedures, SOPs)
- Human resources and training
- Communication and information exchange
- Infrastructure and equipment

The main cooperating actors are border guards (border police), police, customs, phytosanitary services, veterinary services, foreign affairs, and national security agencies. Focusing on procedures, a simplified model called the “Four-Tier Access Control Model” (sometimes referred to as the four-filter model – see Figure 5) is used, which covers a set of complementary measures implemented at different stages, which include:

1. Activities in third countries (visa policy, liaison officers, assistance missions);
2. International cooperation (readmission treaties, return and other joint operations, FRONTEX, PCC SEE etc.);
3. Border surveillance and inspections at border gates (border check, customs check etc.)
4. Inland checks and other activities within territory.

In line with the ambition of the iCROSS, Section 2.2 focuses on border checks within border control (Filter 3) at external borders of the Schengen Area, highlighting the following aspects:

- (Partial) Automated Border Control (ABC) speeding up border checks with help of biometrics
- Voluntary version of Advanced Passenger Information (API)
- Entry-Exit System (EES)
- Voluntary Registered Traveller Program (RTP)

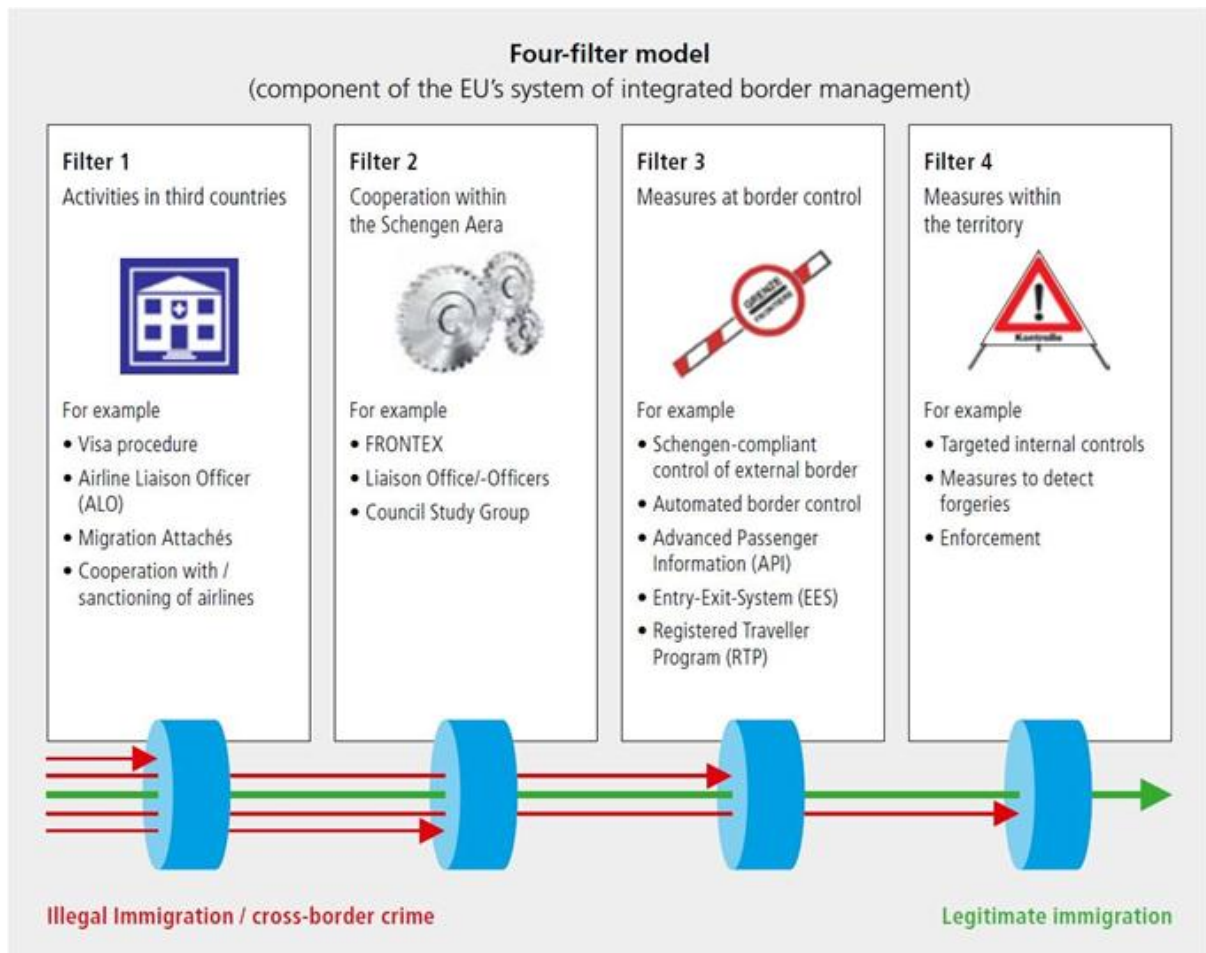


Figure 5 The Four Tier Access Control Model

Although the iCROSS solution is focusing on border checks at border gates, especially at land border gates, it is borne in mind that the given procedure will likely be connected to other procedures in the same tier or in other tiers. For example, a record serving as evidence for border crossing (“digital stamp”) shall be consulted during an inland check to determine if the duration of the stay is exceeded or not. Checks in one tier are the best place to optimize cost effectiveness, e.g. multiple stakeholders conduct checks at the border, like customs, border guards, phytosanitarians etc. Such checks can include (depending on the border section), means of transport, pets brought along, declared belongings etc. Consequently, more checks can be carried out before, after or during the border check itself. For a traveler passing between Hungary and Romania, there is border check but no customs check, while a trip between Hungary and Serbia requires both and in third version, when crossing from Germany to Switzerland, there is customs check but no border check. These checks can be extended by veterinary and phytosanitary checks if necessary. Road Border Crossing Points need a dual check: both vehicles and passengers have to be checked, it has to be verified that

the vehicle is rightfully owned, able to safely participate in the traffic and there is nobody hiding in the vehicle trying to slip across the border without being checked or there are no hidden drugs, weapons, explosives or other illicit goods. Therefore, border checks at land border gates are not only considering control of the passengers, but also inspection of the vehicle in compliance with the Schengen Border Code. The Schengen Border Code applies for border control activities of the Schengen Member States (MS), which is was originally an independent international cooperation (Treaty of Schengen on Abolishing Border Control on Internal Borders, also known as Schengen Agreement signed in 1985) on abolishing border control at the Parties' internal (common) borders. Subsequently, the EU took over this institution of the international law and integrated into the *acquis communautaire* in 1999 with the Treaty of Amsterdam. However, the EU and Schengen Membership did not totally overlap, some EU MS opted out, while some third countries joined the Schengen Area. Figure 6 shows the current Schengen and EU overlap as of 2016.

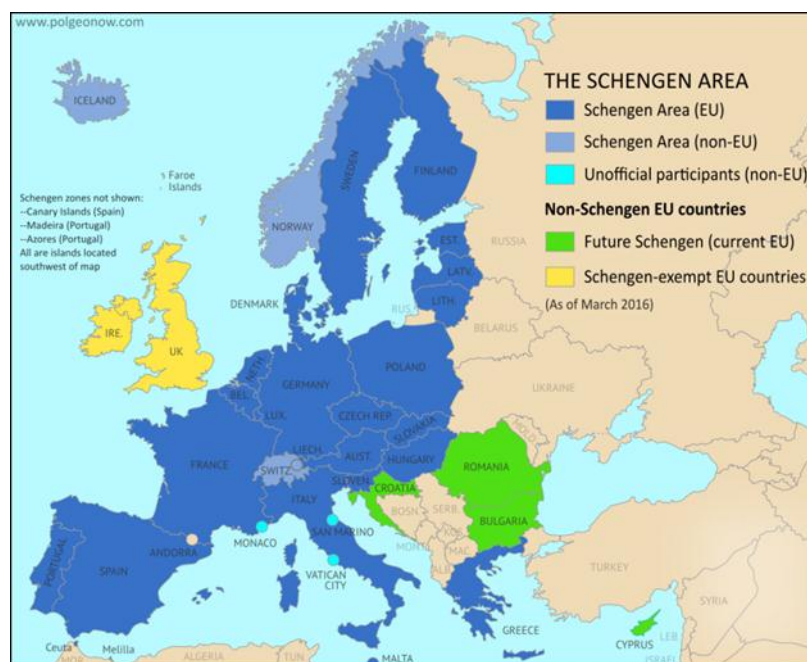


Figure 6 Current Schengen and EU Overlap (2016)

2.5 Border policing

Although IBM is a backbone of border management in the Schengen MSs, border policing is a wider horizontal national institution in each MS, it does include IBM but has dimensions outside of it. They are mostly regulated by bi- or multilateral international agreements between countries. There is a long standing effort from the EU to get involved into – and later, take over – all aspects of border policing from the MS. In some cases, for example in case of readmission treaties with third countries or visa policy, under Cross-Border Relations, this is very much reasonable. On the other hand, a border regime, which is a bilaterally agreed regime of the border area of two neighboring countries, is more of a subsidiary and is less justifiably centralized.

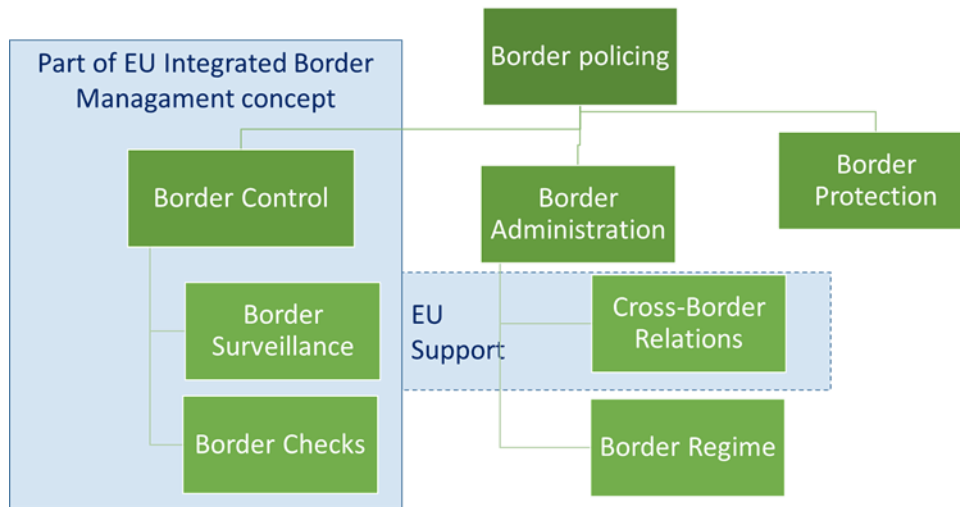


Figure 7 EU Intergrated Border Management Concept

However, it has to be respected, that border policing is a part of the flow control of persons, goods and services (see Figure 8). It is a pillar of the National Security System of each MS, which has not only law-enforcement or foreign affairs aspects, but other ones from sanitation through labour market to national security, even if the filter itself is the Four-Tier Access Control Model (4-TAC) of the IBM.

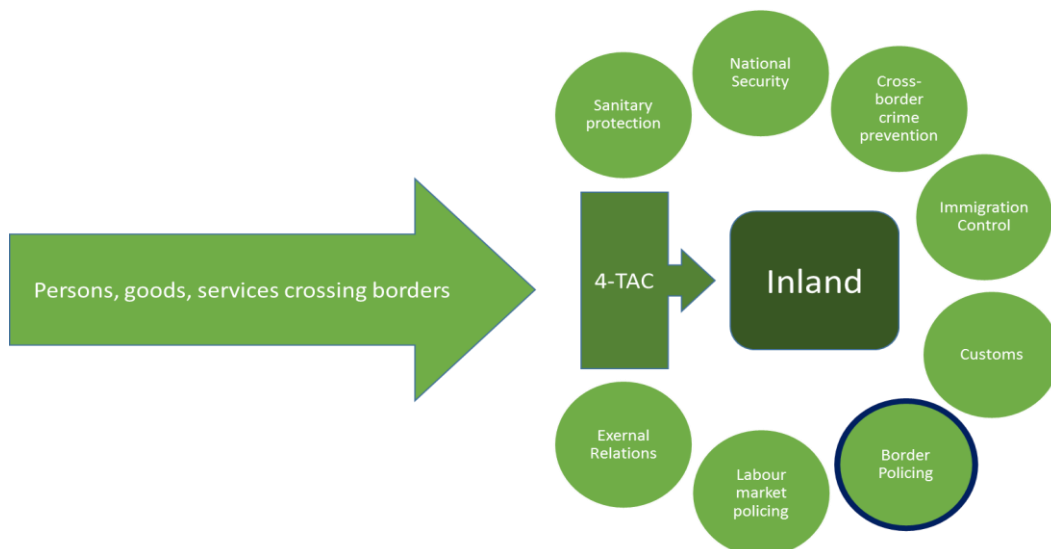


Figure 8 Border Policing Flow

2.6 Basic definitions and principles of border control

Border control consists of border surveillance and border checks at external borders. **Border surveillance** means the surveillance of borders between border crossing points and the surveillance of border crossing points outside the fixed opening hours, in order to prevent persons from circumventing border checks. **Border checks** are the checks carried out at border crossing points at the external border, to ensure that persons, including their means of transport and the objects in their possession, may be authorized to enter the territory of the Member States or

authorized to leave it. **External borders** means the Member States' land borders, including river and lake borders, sea borders and their airports, river ports, sea ports and lake ports, provided that they are not internal borders. **Internal borders** means the common land borders, including river and lake borders, of the Member States; the airports of the Member States for internal flights; sea, river and lake ports of the Member States for regular internal ferry connections (Regulation (EU) 2016/399 on Schengen Borders Code, Art. 2.). External borders may be crossed only at border crossing points and during the fixed opening hours. Internal borders may be crossed at any point without a border check on persons, irrespective of their nationality, being carried out. A summary is presented in Table 1.

Table 1 Border Types and Associated Border Checks

Border type	Border Checks
Schengen external border	Yes
Schengen internal border	No
Schengen internal border with temporary re-established border control	Yes
Schengen external border during temporary border openings	No
Schengen external borders with relaxed border checks	Simplified
Closed border (protected border)	No (no traffic)

Cross-border movement at external borders shall be subject to checks by border guards. Checks shall be carried out in accordance with the Schengen Borders Code, but the law of the Member State concerned shall apply to any searches which are carried out. The border checks may also cover the means of transport and objects in the possession of the persons crossing the border.

All persons shall undergo a **minimum check** in order to establish their identities on the basis of the production or presentation of their travel documents. Such a **minimum check** shall consist of a rapid and straightforward verification, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document authorizing the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting. On a non-systematic basis, when carrying out minimum checks on persons enjoying the right of free movement under Union law, border guards may consult national and European databases in order to ensure that such persons do not represent a genuine, present and sufficiently serious threat to the internal security, public policy, international relations of the Member States or a threat to the public health.

On entry and exit, third-country nationals shall be subject to **thorough checks (first line)** containing a minimum check plus verification of the conditions of entry and stay for third country nationals.

Figure 9 Border Checks, shows a summary of the three levels of checks.

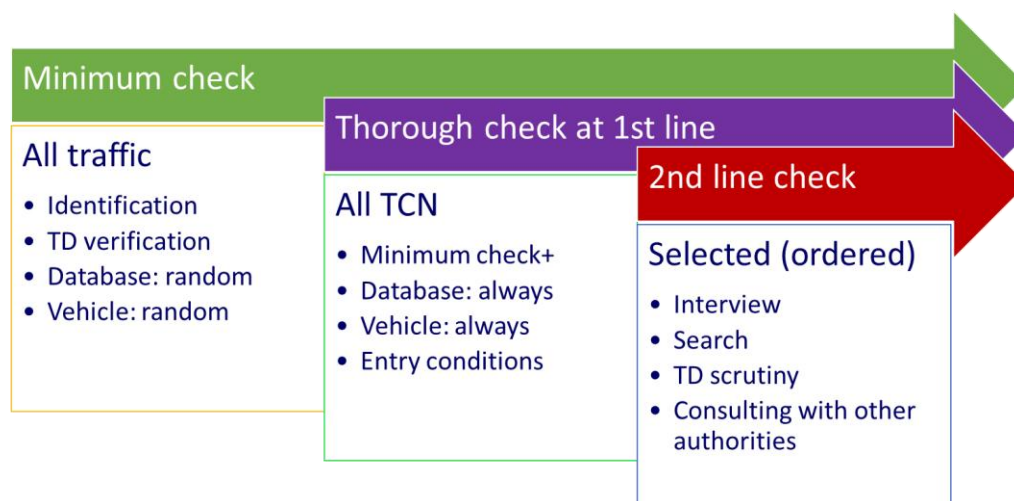


Figure 9 Border Checks

If a third country national stays less than 90 days in any 180 days period, the conditions for entry and stay in the Schengen Code has to be applied. If a person stays more than 90 days in any 180 days period, the immigration law of the Members State shall be applied.

During a thorough check, the following procedure is requested by the Schengen Border Code:

1. verification that a third-country national is the rightful holder of a document which is valid for crossing the border and which has not expired, and that the document is accompanied, where applicable, by the requisite visa or residence permit;
2. thorough scrutiny of the travel document for signs of falsification or counterfeiting;
3. examination of the entry and exit stamps on the travel document of the third-country national concerned, in order to verify, by comparing the dates of entry and exit, that the person has not already exceeded the maximum duration of authorized stay in the territory of the Member States;
4. verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay, checking, if necessary, the corresponding supporting documents;
5. verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully;
6. verification that a third-country national, his or her means of transport and the objects he or she is transporting are not likely to jeopardize the public policy, internal security, public health or international relations of any of the Member States. Such a verification shall include direct consultation of the existing (if any) data and alerts on persons, included in the SIS and in national data files as well as the corresponding action to be performed, as a result of an alert;
7. if a third country national needs a visa, verification of the visa holder identity and visa authenticity is done by consulting the Visa Information System (VIS), but this can be skipped under certain special circumstances: e.g. disaster, person is part of a diplomatic delegation led by a Head of State.

8. the travel documents of third-country nationals shall be systematically stamped on entry and exit.

For intended stays on the territory of the Member States of a duration of no more than 90 days in any 180-day period, which entails considering the 180-day period preceding each day of stay, the entry conditions for third-country nationals are the following:

1. rightful possession of a valid travel document entitling the holder to cross the border satisfying the following criteria:

1.1. its validity shall extend at least three months after the intended date of departure from the territory of the Member States. In a justified case of emergency, this obligation may be waived;

1.2. it should have been issued within the previous 10 years;

2. they are in possession of a valid visa, if required, except where they hold a valid residence permit or a valid long-stay visa;

3. they justify the purpose and conditions of the intended stay, and they have sufficient means of subsistence, both for the duration of the intended stay and for the return to their country of origin or transit to a third country into which they are certain to be admitted, or are in a position to acquire such means lawfully;

4. they are not persons for whom an alert has been issued in the SIS for the purposes of refusing entry;

5. they are not considered to be a threat to public policy, internal security, public health or the international relations of any of the Member States, in particular where no alert has been issued in Member States' national data bases for the purposes of refusing entry on the same grounds.

In the Schengen Border Code, there are also special rules on border checks at land border gates. To ensure effective checks on persons, while ensuring the safety and smooth flow of road traffic, movements at border crossing points shall be regulated in an appropriate manner. Where necessary, MSs may conclude bilateral agreements to channel and block traffic. At land borders, MSs may, where they deem appropriate and if circumstances allow, install or operate separate lanes at certain border crossing points. For example, in Hungary, there are separated lanes for persons under the right of free movement and stay ('EU Citizens') and third country nationals ('All Passports'), as well as for busses and trucks and – on larger border gates – for diplomats. Separate lanes may be dispensed with at any time by the MSs' competent authorities, in exceptional circumstances and where traffic and infrastructure conditions so require. As a general rule, persons travelling in vehicles may remain inside them during checks. However, during the first line check, if circumstances so require, persons may be requested to alight from their vehicles. Thorough checks will be carried out, in areas designated for that purpose, if local circumstances allow. In the interests of staff safety, checks will be carried out, where possible, by two border guards.

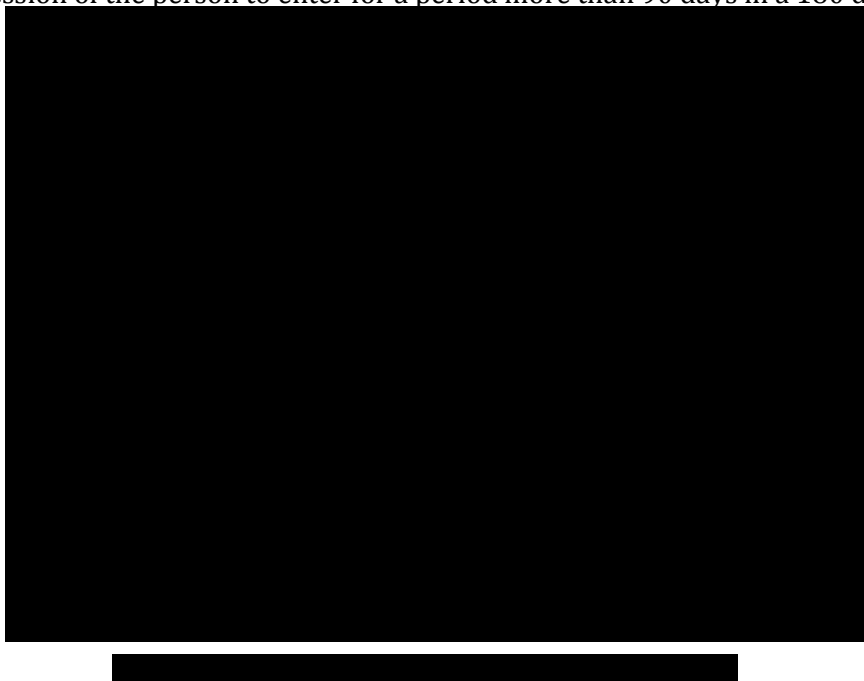
2.7 Border checks in Hungary

For an intended stay on the territory of Hungary for more than 90 days in any 180 days period, in case of persons under the right of free movement and stay [the Act I. of 2007](#), for third country citizens the [Act II. of 2007](#) shall be applied.

In the case above, persons under the right of free movement and stay are required to present a registration card issued by the Hungarian Office of Immigration and Nationality or, if not (yet)

holding this, to present documents justifying their right of free movement and stay for more than 90 day in a 180 days period, for example a certificate of marriage with a person residing in Hungary, a Hungarian Student's Card or a work contract. If the person is a third country national, obtained the right of free movement and stay through marriage or other family relationship, a residence permit will also be required or, if not (yet) in possession of the person, but based on nationality, a visa is required to enter, a visa free of charge will be issued immediately.

For third country nationals not under the right of free movement and stay, a residence permit (temporary or permanent) or visa issued for the special purpose of obtaining a residence has to be in rightful possession of the person to enter for a period more than 90 days in a 180 days period.



2.7.1 Detailed procedure of border checks in Hungary

The Hungarian procedure on carrying out border checks at land border gates is regulated by [Command No. 24/2015 of the Chief Commissioner](#). According to this, the following steps have to be carried out:

1. Minimum checks:
 - 1.1. observation of the arriving vehicle
 - 1.2. greeting the passengers (language knowledge check based on vehicle plate)
 - 1.3. taking travel document, verification of its type (ordinary [private], service, diplomatic, ID or is not valid as a travel document [eg. driving license])
 - 1.4. verification of the nationality and the right of free movement and stay
 - 1.5. identification of the holder of the passport (impostor check)
 - 1.6. verification of presence of persons in the passport

-
- 1.7. verification of the vehicle, its cargo bays and other holding spaces (trunk, door, under seat and overhead compartments and engine bay if necessary), vehicle license, ownership and the right to use (e.g. power of attorney if the driver is not direct relative of the owner), operational condition of the vehicle, vehicle insurance and driver license (if required)
 - 1.8. checking passport and its annexes for validity and genuineness
 - 1.9. non-systematic check of person, vehicle and travel document in relevant databases using the single HERR (Határ Ellenőrző és Regisztrációs Rendszer (System for Entry-Exit and Border Checks)) form (there are 18 cases when the check is obligatory, e.g. when any traveller is underage and without guardian)
 - 1.10. recording statistical data such as number of persons, nationality of persons and means of travel.
 - 1.11. giving back the travel documents to the holders (one by one) after repeated identification
 - 1.12. decision
 2. Decisions of minimum check can be:
 - 2.1. admission
 - 2.2. thorough check at first line
 - 2.3. thorough check at second line
 - 2.4. refusal
 - 2.5. actions according to hit in Schengen Information System, SIS
 - 2.6. further actions are required (apprehension, arrest, starting of asylum, criminal, immigration etc. procedure)
 3. Thorough checks at first line:
 - 3.1. observation of the arriving vehicle
 - 3.2. greeting the passengers (language knowledge check based on vehicle plate)
 - 3.3. taking travel document, verification of its type (ordinary [private], service, diplomatic, ID or is not valid as a travel document [e.g. driving license])
 - 3.4. verification of the nationality and the necessity of visa
 - 3.5. identification of the holder of the passport (impostor check)
 - 3.6. verification of presence of persons in the passport
 - 3.7. verification of the vehicle, its cargo bays and other holding spaces (trunk, door, under seat and overhead compartments and engine bay if necessary), vehicle license, ownership and right to use (e.g. power of attorney if the driver is not direct relative of the owner), operational condition of the vehicle, vehicle insurance and driver license (if required)
 - 3.8. checking passport and its annexes for validity and genuineness

3.9. in case the person requires a visa, checking possession of visa or other document replacing the visa

3.10. check of person, vehicle and travel document (passport, visa etc.) in relevant databases using the single HERR form, checking fingerprints if required by VIS

3.11. verifying conditions for entry and stay, with focus on the threat to public order and national security posed by the person, its vehicle or any objects in its possession

3.12. checking official remarks and stamps in the travel document

3.13. verifying if the person has not exceeded the maximum duration of stay he or she is eligible for

3.14. stamping the travel document and additional remarks if required (e.g. +00256797 if the person shall have a visa by nationality but instead has a residence permit with that number)

3.15. recording statistical data

3.16. giving back the travel documents to the holders (one by one) after repeated identification

3.17. decision

4. Decisions of the Minimum check can be

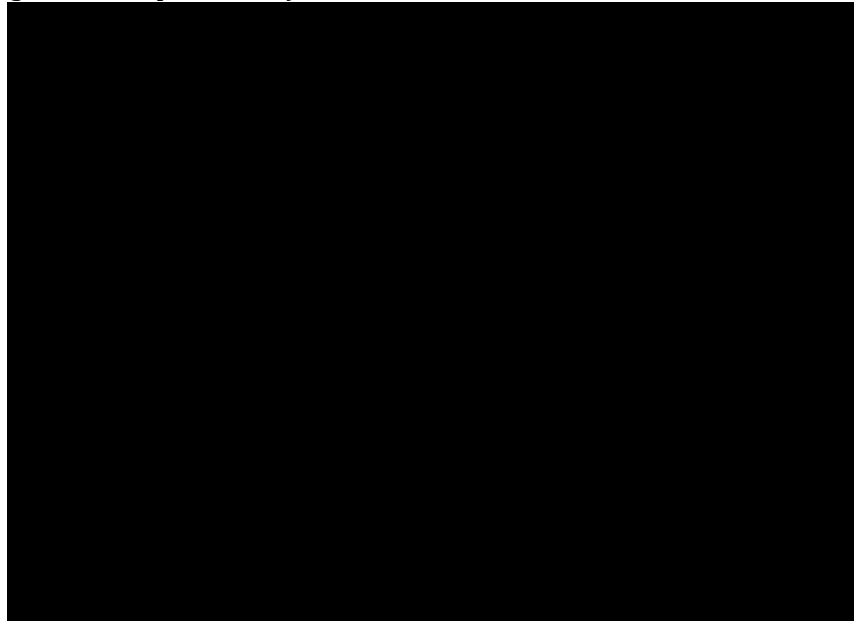
4.1. admission

4.2. thorough check at second line

4.3. refusal

4.4. actions according to hit in SIS

4.5. further actions are required (apprehension, arrest, starting of asylum, criminal, immigration etc. procedure)



2.7.2 Databases used during border check

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

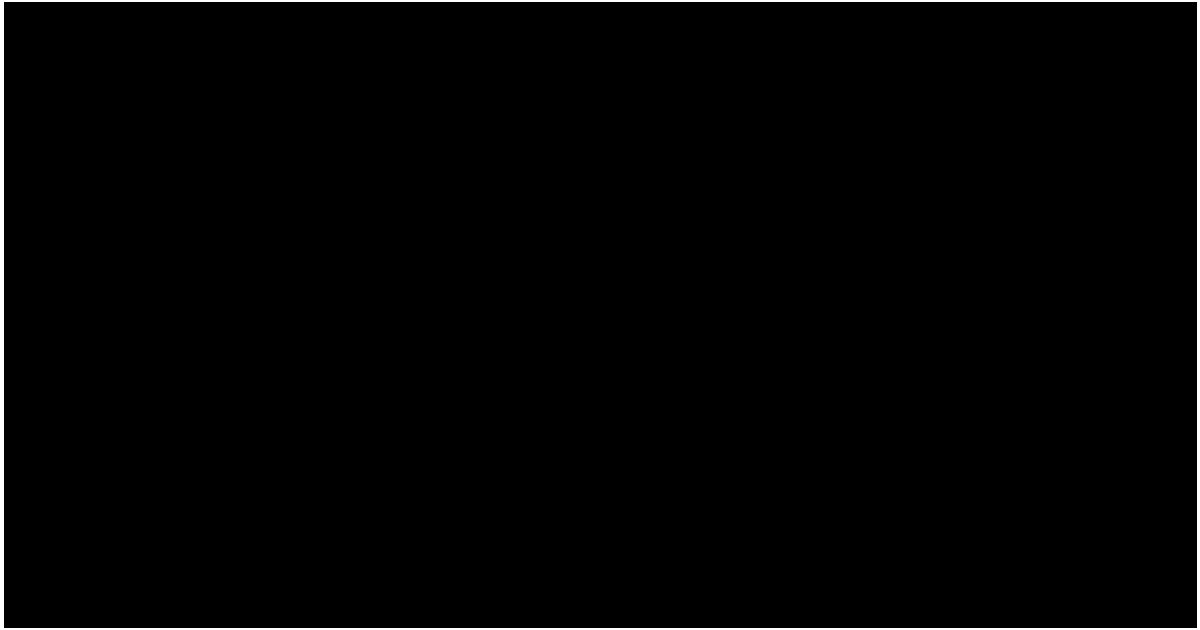
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

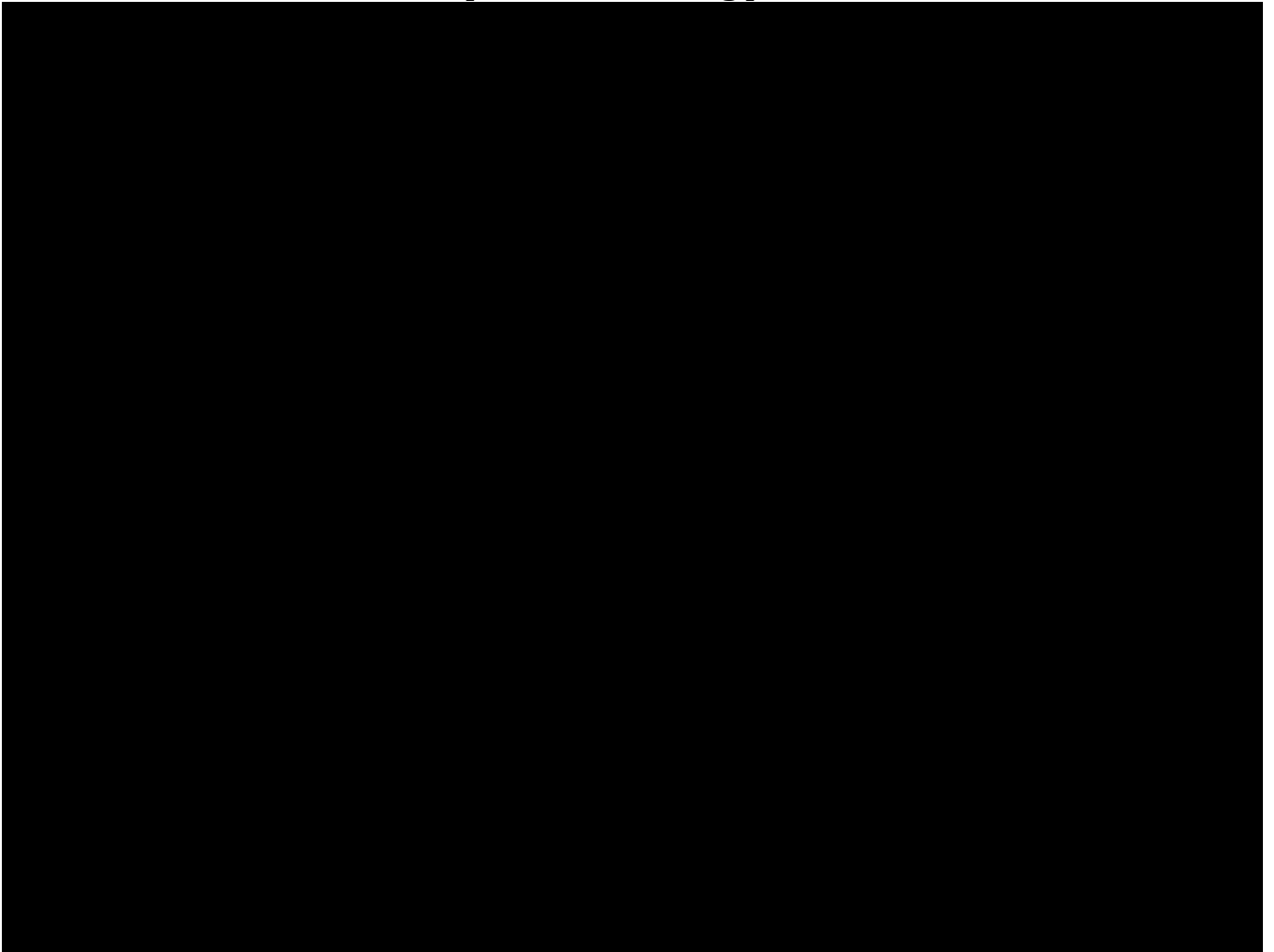
[REDACTED]

[REDACTED]

[REDACTED]



2.7.3 Comparison of existing products features



2.8 Republic of Latvia

The State Border Guard ensures surveillance of the 276 km long border between the Republic of Latvia and Russian Federation, the 172,9 km long border between the Republic of Latvia and the Republic of Belarus, and the 498 km long sea border (external EU border), as well as monitoring of the 343 km long border between the Republic of Latvia and the Republic of Estonia and the 588 km long border between the Republic of Latvia and the Republic of Lithuania (internal EU border).

At the state borders with the Russian Federation and with the Republic of Belarus there are 6 border crossing points located on motorways and 3 border crossing points on railways. 10 border crossing points are located in ports and 6 in airports and airfields.

The main tasks of the Border Guard include:

1. Border check of persons and means of transport at BCP;
2. Surveillance of the land and sea border between BCP;
3. Control of foreigners residence into the country and expulsion of illegal migrants (immigration control);
4. Investigation of criminal cases on illegal crossing of the state border and people illegal movement ;

5. Identification of asylum seekers;
6. Technical documents' expertise.

Rights of Border Guards

Border guards in the whole border area, as well as the border control points and the border crossing points have the right:

1. to examine the documents of persons and control means of transport and their freight, during the performance of their service duty without limitations of movement;
2. for all persons crossing the State border, to examine according to specified procedures personal identification documents and make the necessary notations in them, as well as to carry out inspections of all the means of transport crossing the State border;
3. in accordance with procedures and within the terms set out by law to arrest persons;
4. to guard, convey and hold arrested persons;
5. in accordance with specified procedures, to remove and transfer to customs institutions goods and other items that have been found with persons crossing the State border while evading customs control;
6. to deny entry into the State to persons who cannot produce valid travel documents;
7. in accordance with procedures prescribed by law, to expel persons from the State who have entered Latvia or crossed the State border without a valid travel document or a permit from the relevant authority or have not observed prescribed procedures;

Organisation of Border Control at Border Crossing Points and at the State Border

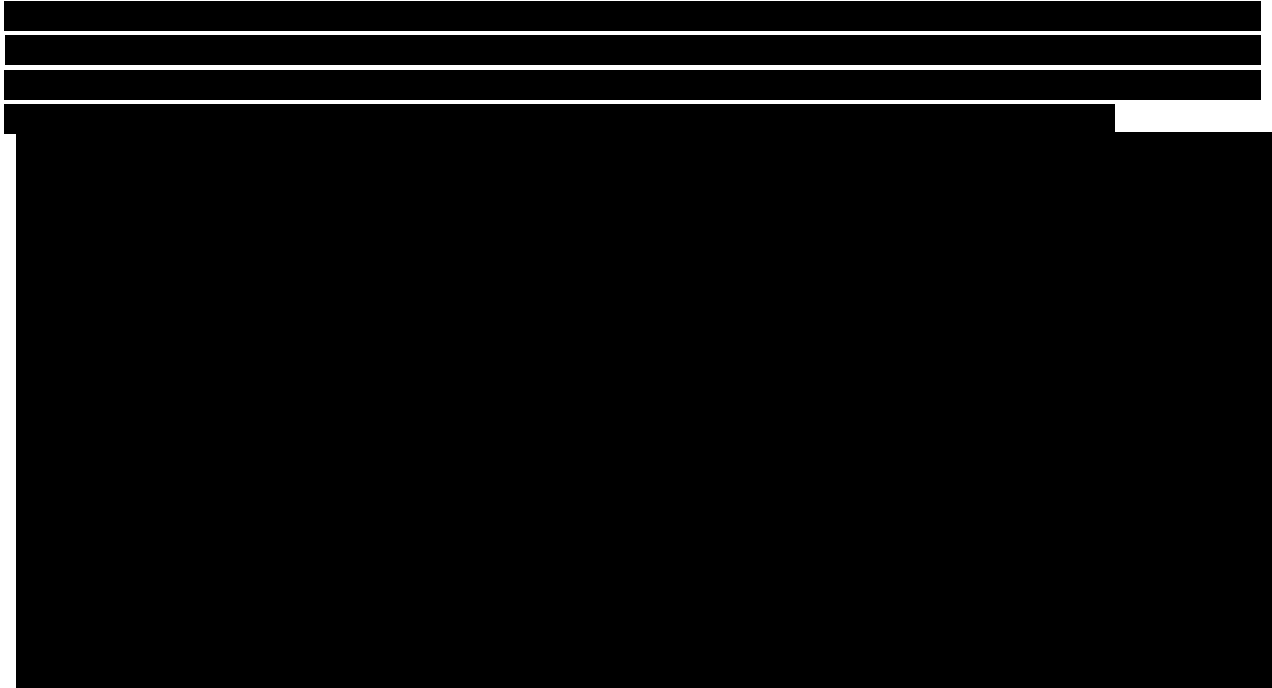
Persons crossing the external border in order to enter or exit the Republic of Latvia, as well as property and goods being moved across the external border by land, by aircraft or vessels in order to bring them into or bring them out of the Republic of Latvia, shall be subject to checks at the border crossing points. The purpose of these checks shall be to confirm the fact of the crossing of the external border and that the persons remain in the Republic of Latvia legally, and that property and goods are being brought into or brought out of the Republic of Latvia legally.

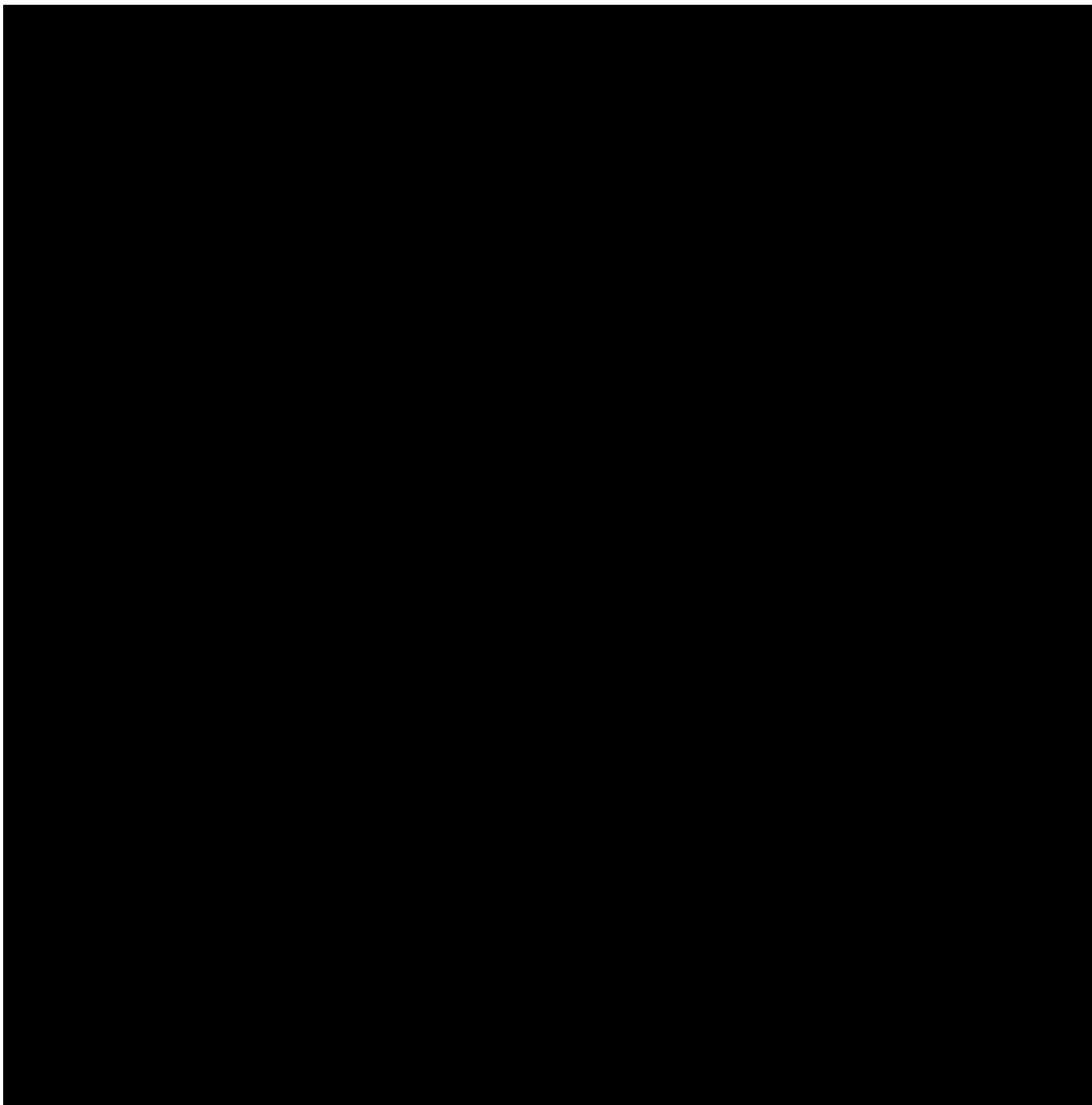
Checks at a border crossing point shall be as follows: the border check, which is performed by officials of the State Border Guard; customs control, which is performed by officials of the customs authority; veterinary or phytosanitary control, control of food safety or of safety of non-food products, quality and classification control, which is performed by officials of the Food and Veterinary Service. Alsoradiometric control, which is performed by officials of State administrative institutions specified in regulatory enactments

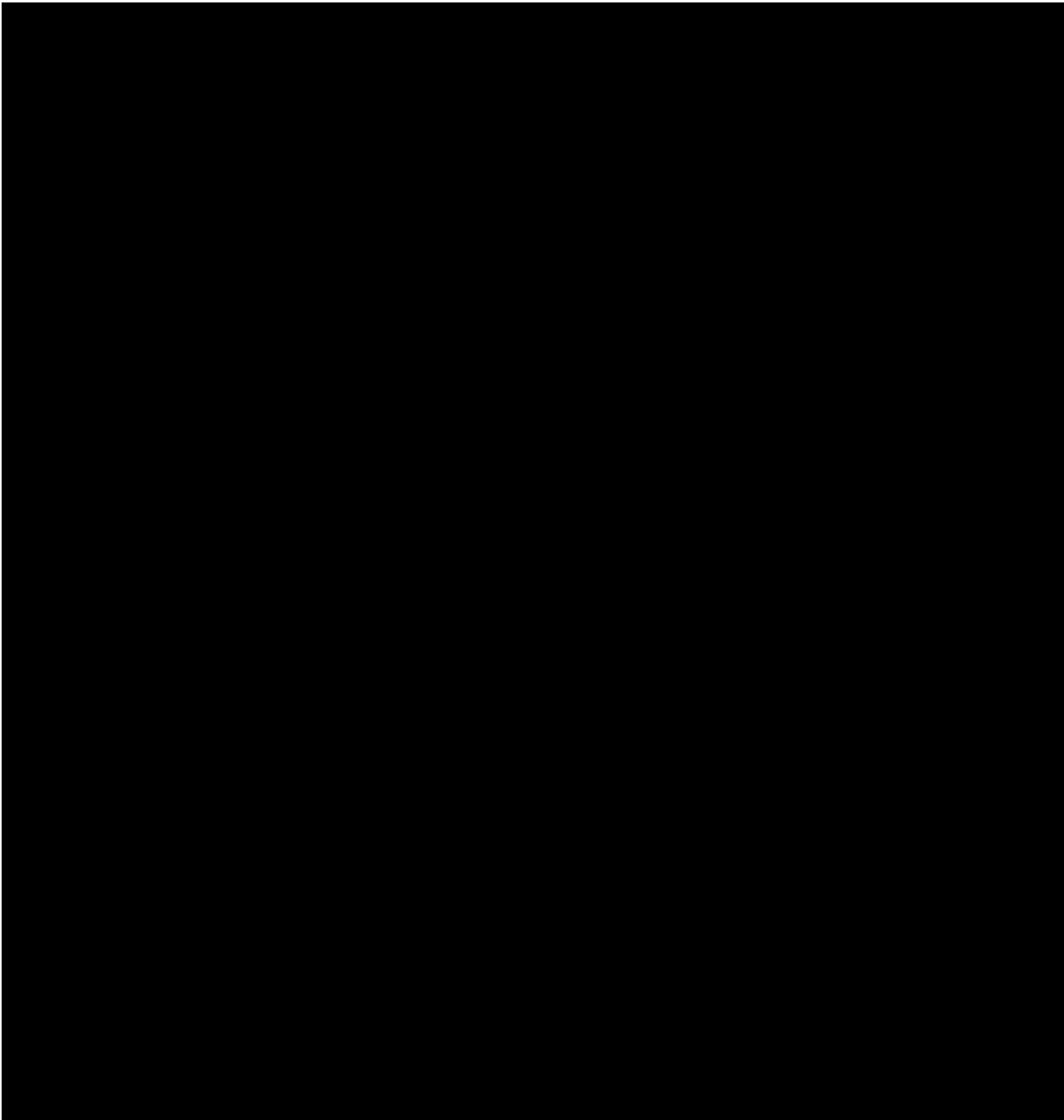
A border crossing point regime shall be in force at border crossing points, which determines the procedures by which persons are permitted to stay and move at a border crossing point, as well as the procedures by which the competent authorities perform activities which are connected with the admittance of persons, as well as the movement of property and goods across the external border.

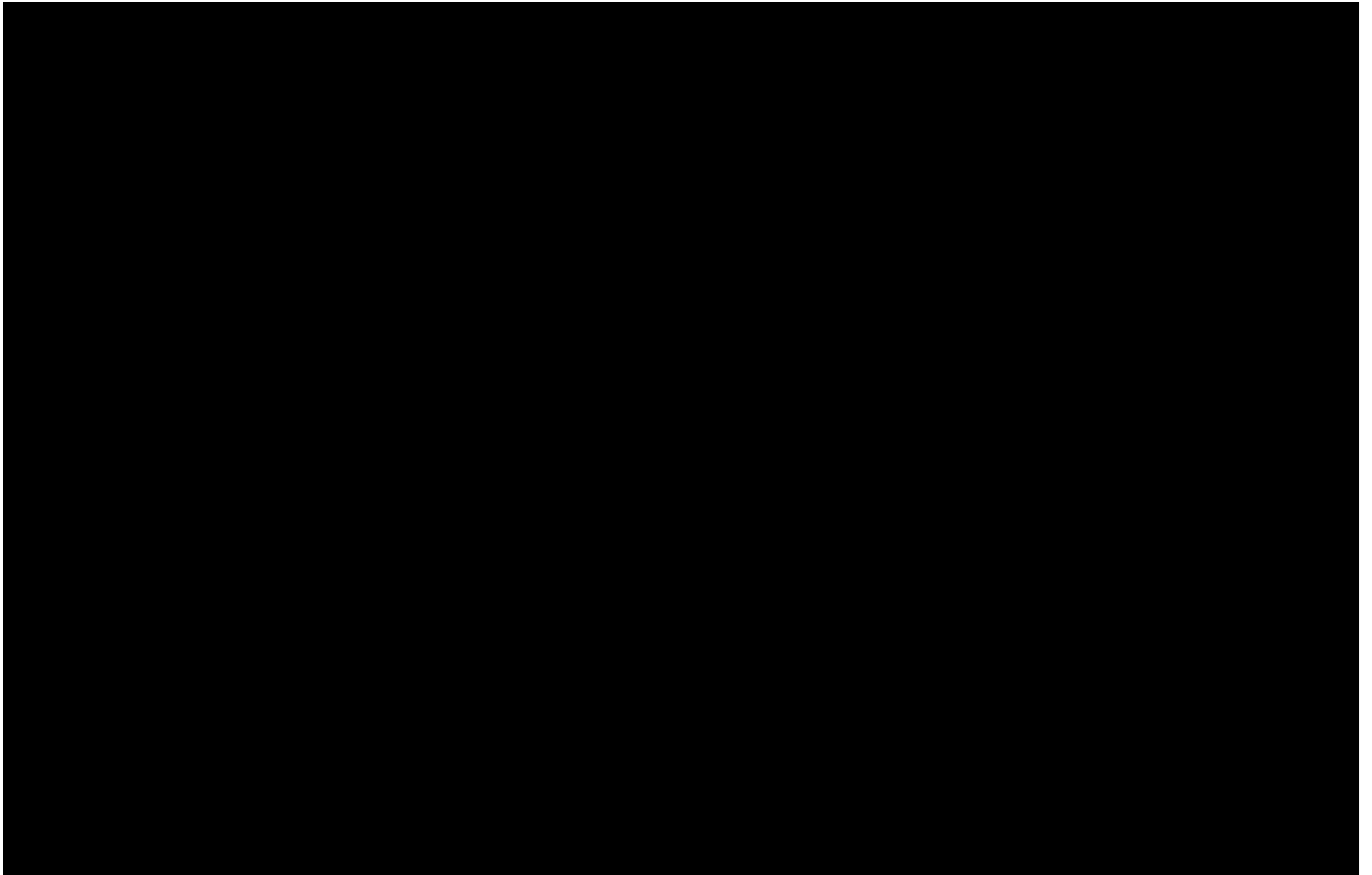
2.8.1 Border check procedure at the Terehova BCP











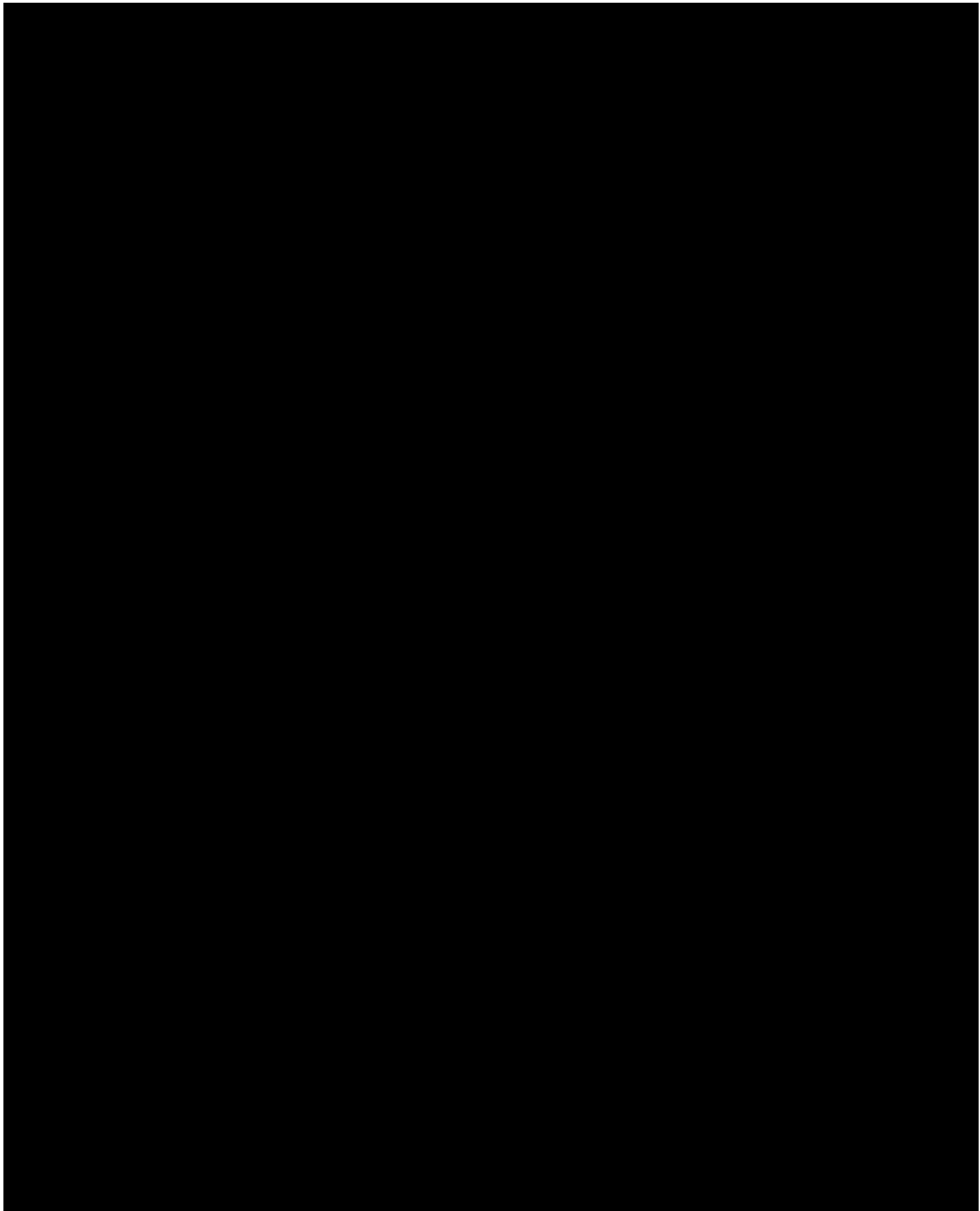
2.8.2 Border check procedure of the Zilupe BCP (railway)

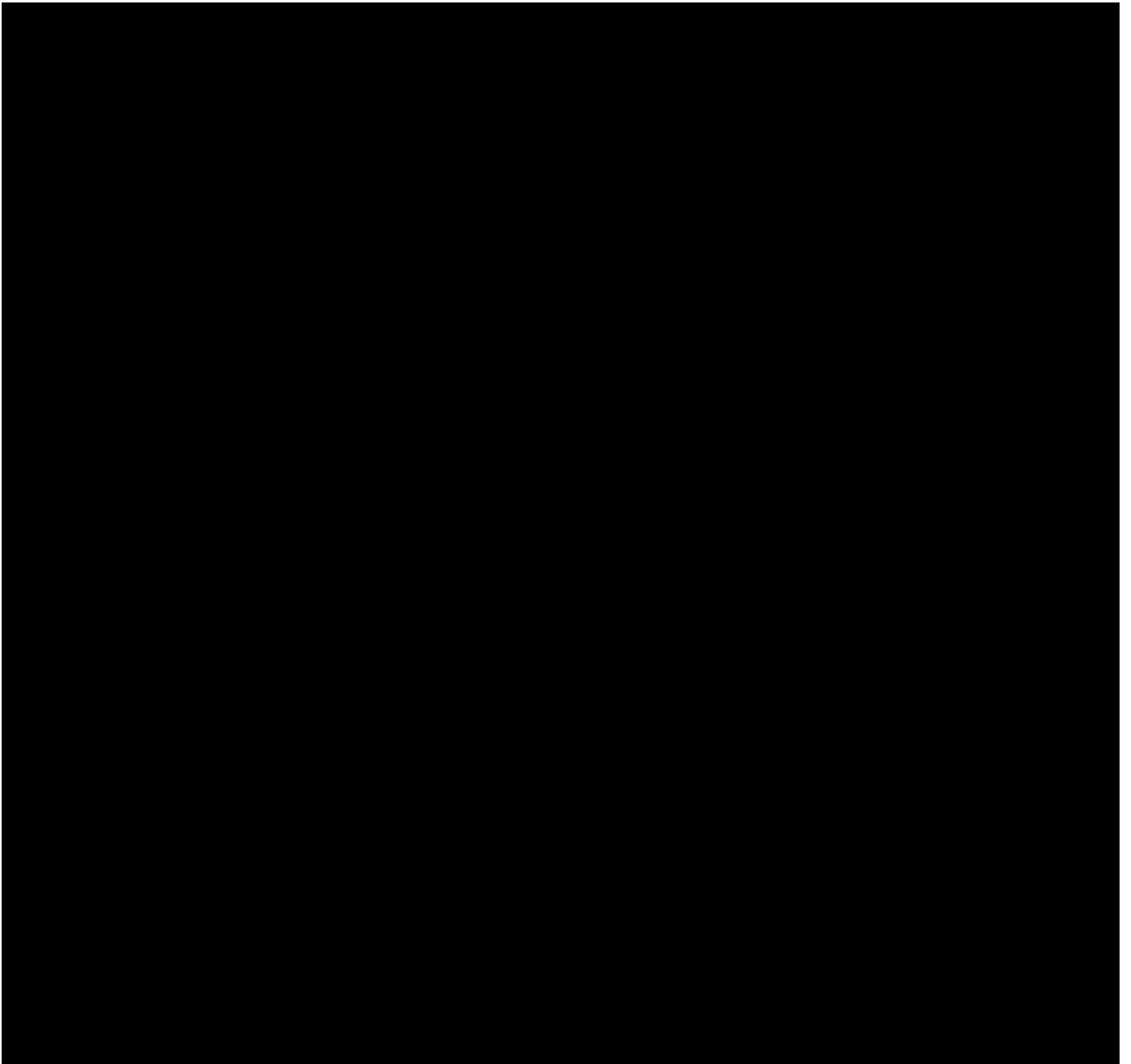
[Redacted text block]

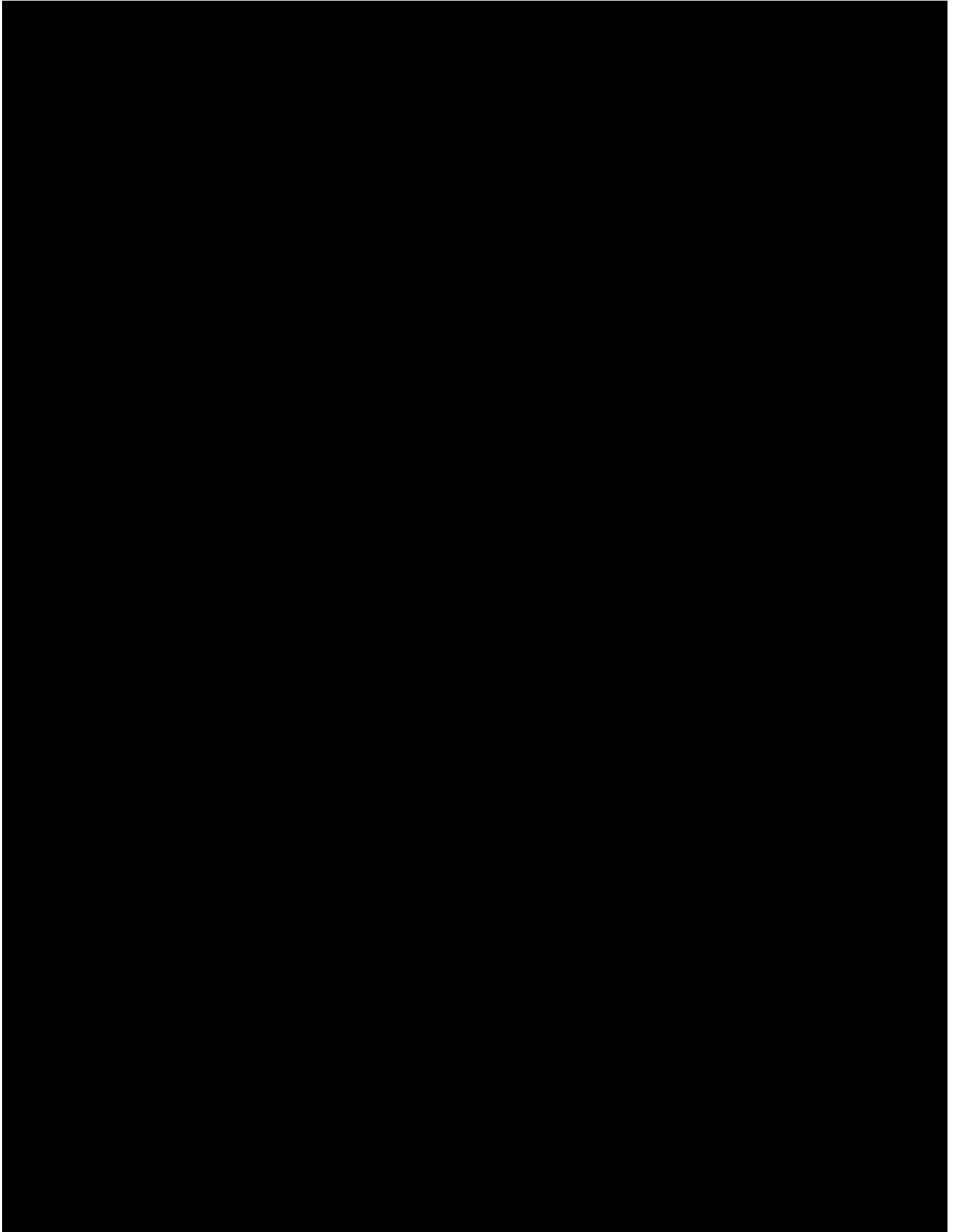
[Redacted text block]

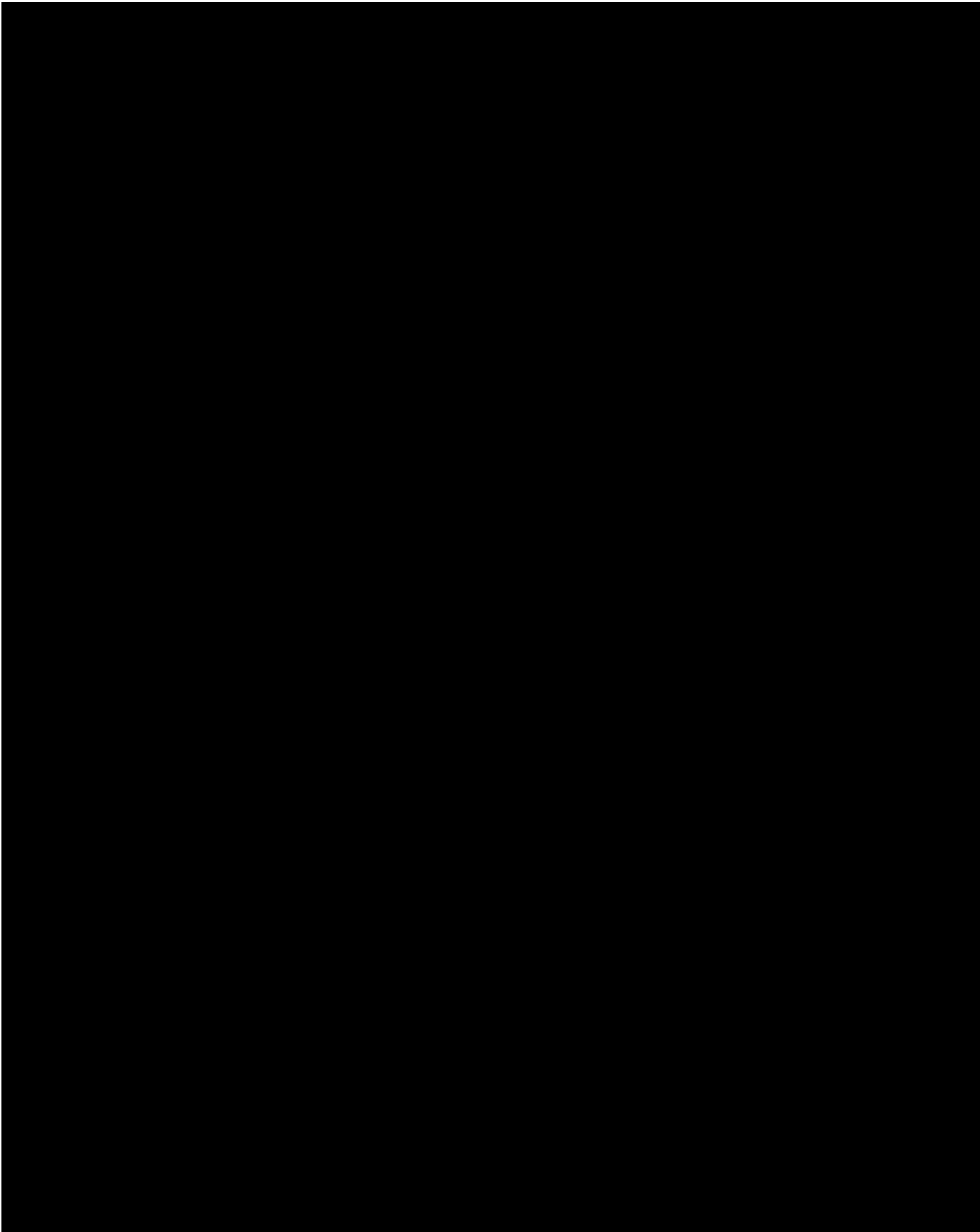
[Redacted text block]

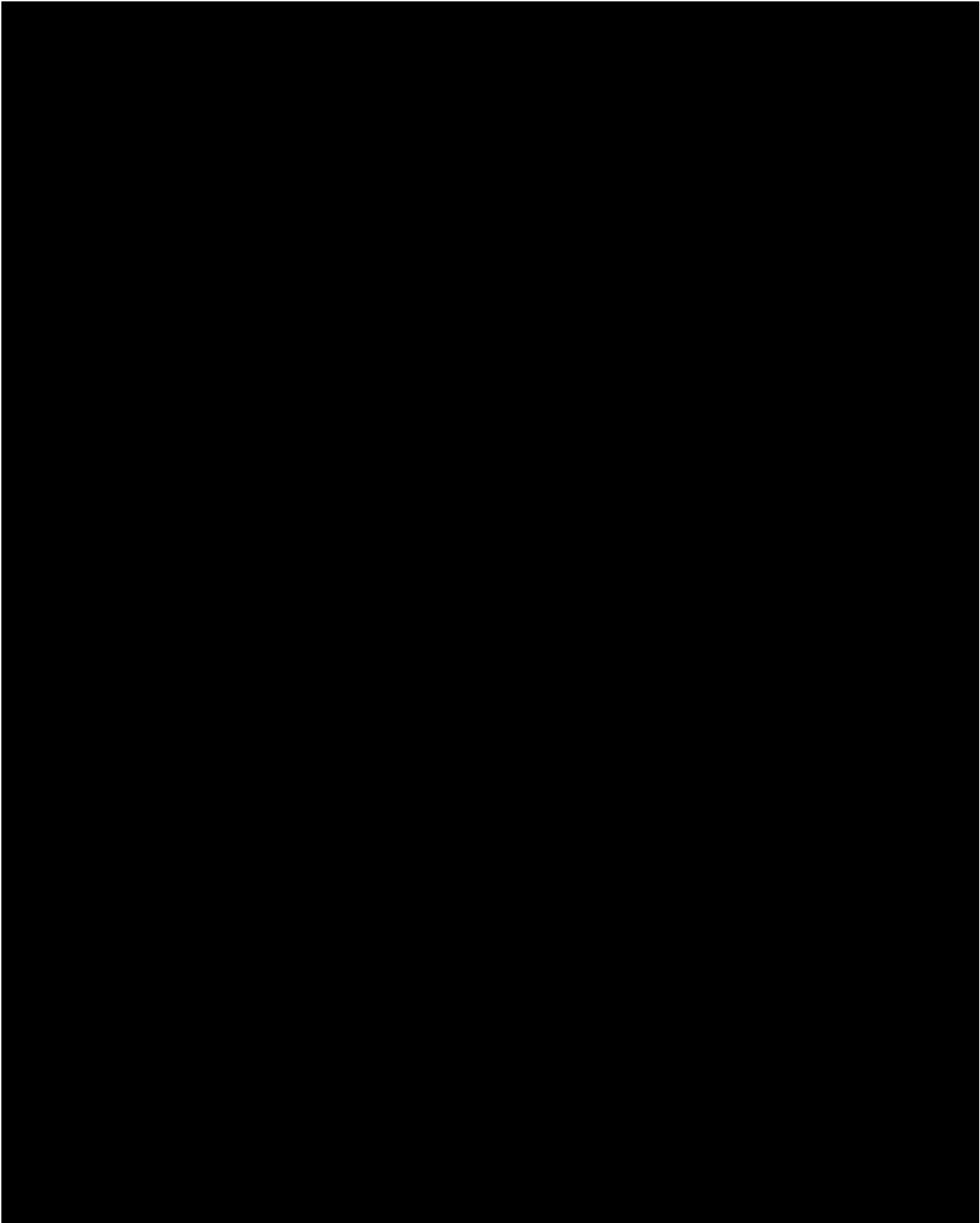
[Redacted text block]

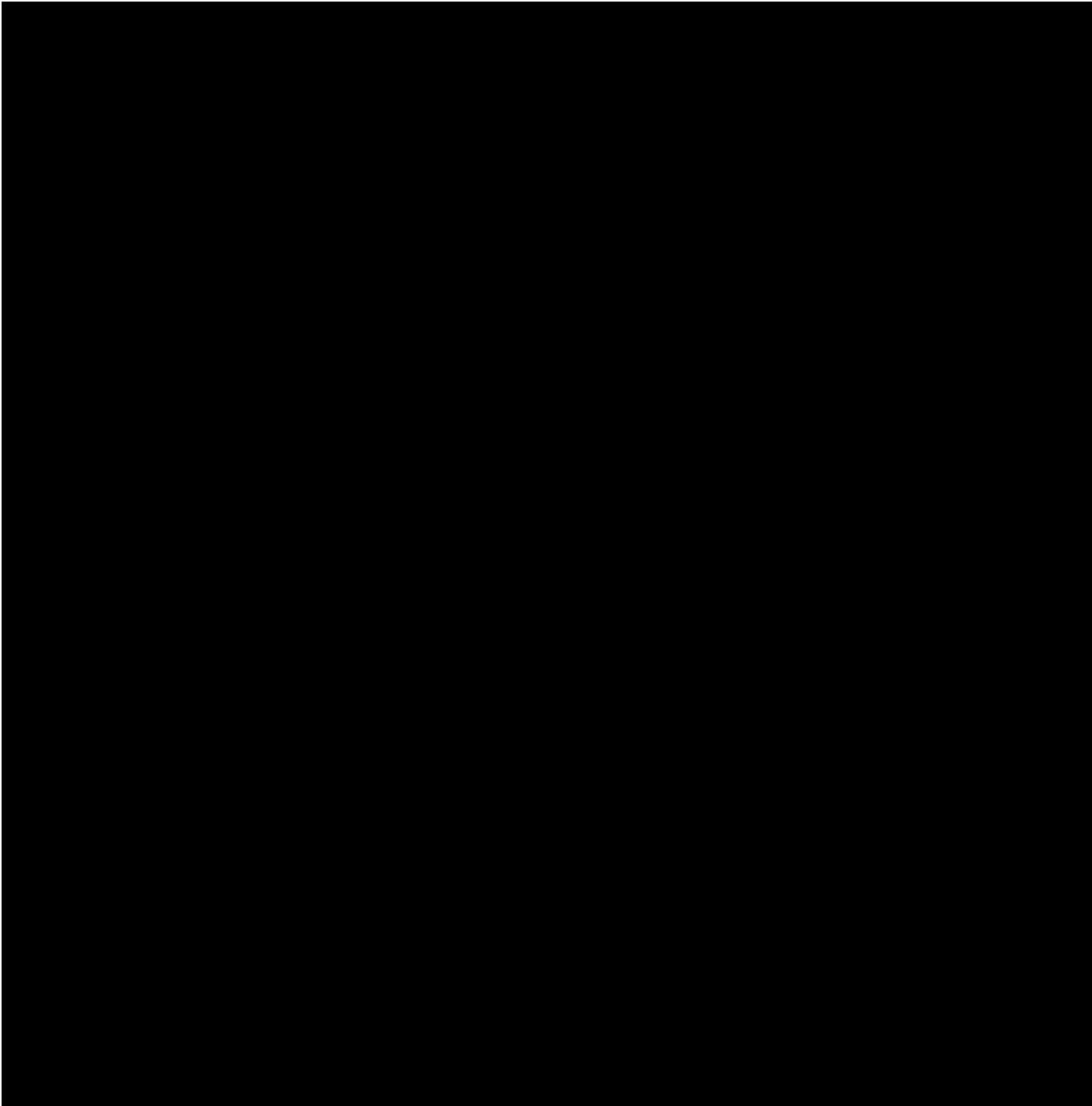






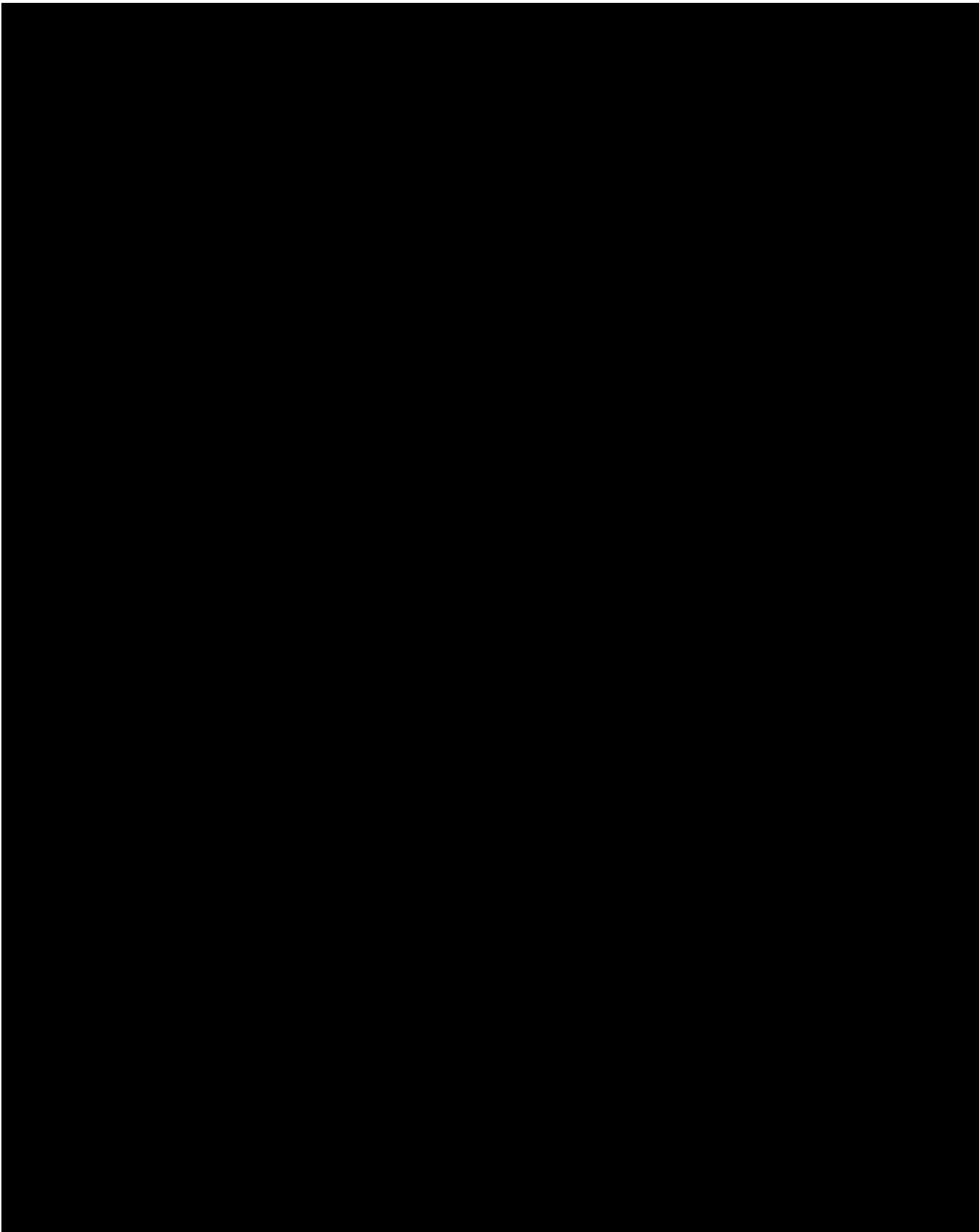






2.8.3 Comparison of existing products features

[Redacted]	
[Redacted]	
[Redacted]	
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]



2.9 TRAINOSE

TRAINOSE S.A. was established on 19th December 2005 as a 100 % subsidiary of OSE S.A. The Hellenic Railways Organization (OSE) is the Greek national railway company which owns, maintains and operates all railway infrastructure in Greece with the exception of Athens' rapid transit lines. Train services on these lines are run by TrainOSE S.A., a former OSE subsidiary. In addition, OSE owns and maintains the rolling stock used by TrainOSE and maintains preserved special rolling stock, withdrawn locomotives and railcars. OSE was founded in 1971, taking over from the Hellenic State Railways, which was founded in 1920. Since 1st January 2007, TRAINOSE S.A. has undertaken the operation and management of all the transportation activities (passenger, freight, etc.) and has been operated as an independent company, being separately managed and organized, according to the provisions of EU legislation.

2.9.1 The Thessaloniki – Eidomeni route

Figure 20 presents a map that shows the position of railway lines within the Greek regions.



Figure 20 Local map of Railway Network

The First line connects Thessaloniki with Istanbul. This route is a part of the corridor that connects west Europe with Asia. The second line connects Thessaloniki with Bulgaria. This route operates with passengers that go to Sofia and freight heading towards the Black Sea and Russia. It is a part of European freight Corridor IV.

The most interesting route, Hellenic – Europe rail transportation, is the Thessaloniki Eidomeni passage. Thessaloniki Eidomeni is the most interesting because:

- It is the main freight corridor of Greek region
- It is the shortest path for immigrants to European Union
- Corridor passes from countries outside EU

The Eidomeni passage connects Thessaloniki with FYROM and is the main freight corridor for Port of Piraeus freight. The Thessaloniki – Eidomeni route is single line electrified route. It operates under high voltage (150KV/25KV, 50HZ) and it holds electrified trains. Electric and Diesel locomotives can operate in this line.

The Electric Multiple Unit (EMU) type of locomotive is for passenger and freight trains. Different types of Diesel and DMU can operate in the line.

2.9.2 Procedures in passenger trains

TRAINOSE is not responsible for checking passenger personal data. According to the Convention concerning International Carriage by Rail, COTIF1999, passengers have the ability to buy a ticket from the central station and travel to the Hellenic Region. (OTIF 1999).

Moreover, TRAINOSE is not a forwarding company. TRAINOSE operates in the Hellenic region. For international travellers, TRAINOSE has bilateral contracts.

Since 10th May 2014, TRAINOSE offers travel from Thessaloniki – Skopje – Belgrade. The train code is Hellas 334/335. The synthesis of the train consists of four wagons and one electrified locomotive. Moreover, TRAINOSE is not a forwarding company. TRAINOSE operates in Hellenic region. For international travellers, TRAINOSE has a bilateral contract with the neighbouring countries and the respective operators operating in them. In Figure 20 (map) the exact position of railway lines from Greek region to other Skopje railway operator is presented.

From 10th May 2014, TRAINOSE offers travel from Thessaloniki – Skopje – Belgrade. The train code is Hellas 334/335. The synthesis of the train consists of four wagons and one electrified locomotive. More specifically:

- One wagon B type which belongs to TRAINOSE. Wagon code is BMPZ and it has 66 seats
- One wagon B type which belongs to Serbian Railways
- One wagon B type which belongs to FYROM railways
- One D type which belongs to FYROM railways

FYROM railways frequently asks for an additional WLB / BC type wagon. Since 2014, but only for the summer period, passengers have the ability to load their car on the train. For this reason, Serbian Railways uses a DDam wagon. So on this route, trains comprise four to six wagons.

The ticketing system for international routes is not electronic. A passenger must go to the Thessaloniki ticketing depot to buy an international ticket (Figure 21).



Figure 21 Thessalonik Passenger Station

On the Thessaloniki – Eidomeni – Skopje - Belgrade route, travellers can buy tickets from Veles Skopje and Nis, Lapovom Belgrade.

- Since 2014, three types of tickets are available. All of the tickets are harmonized with the latest rules concerning the contract of international carriage of passengers by rail (CIV) from International Rail Transport Committee. Typical handwritten tickets together with their wrappers are shown in Figure 22 and Figure 23.

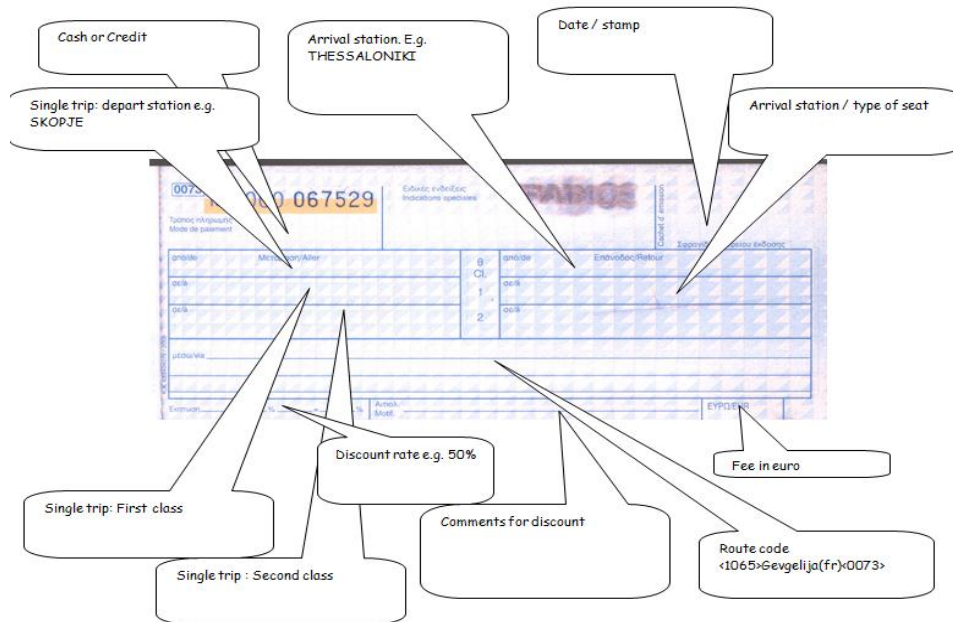


Figure 22 Typical handwritten tickets

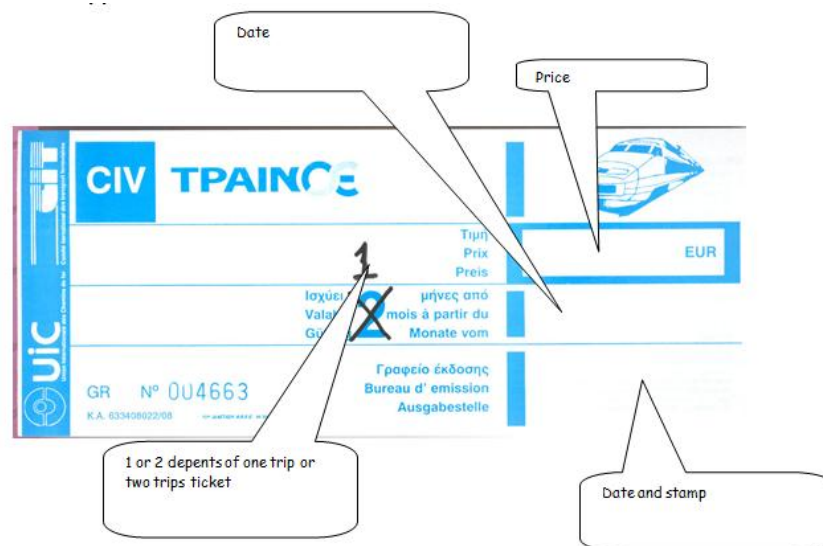


Figure 23 Ticket Wrapper

The conditions of traveling can be found on the back of every wrapper (The International Rail Transport Committee 2015).

After buying a ticket a passenger has to go to the train. The passenger has to find the right wagon and a seat. Inside the wagon, a passenger can put their personal luggage on luggage shelves over their seats.



Figure 26 Typical BMZ Passenger Wagon

The BMZ wagon is a UIC 567-2 wagon (Figure 26, Figure 27). It is a 2nd class wagon with 11 coupes and 2 toilets. It is almost 26.400 mm or 26.4 meters long.

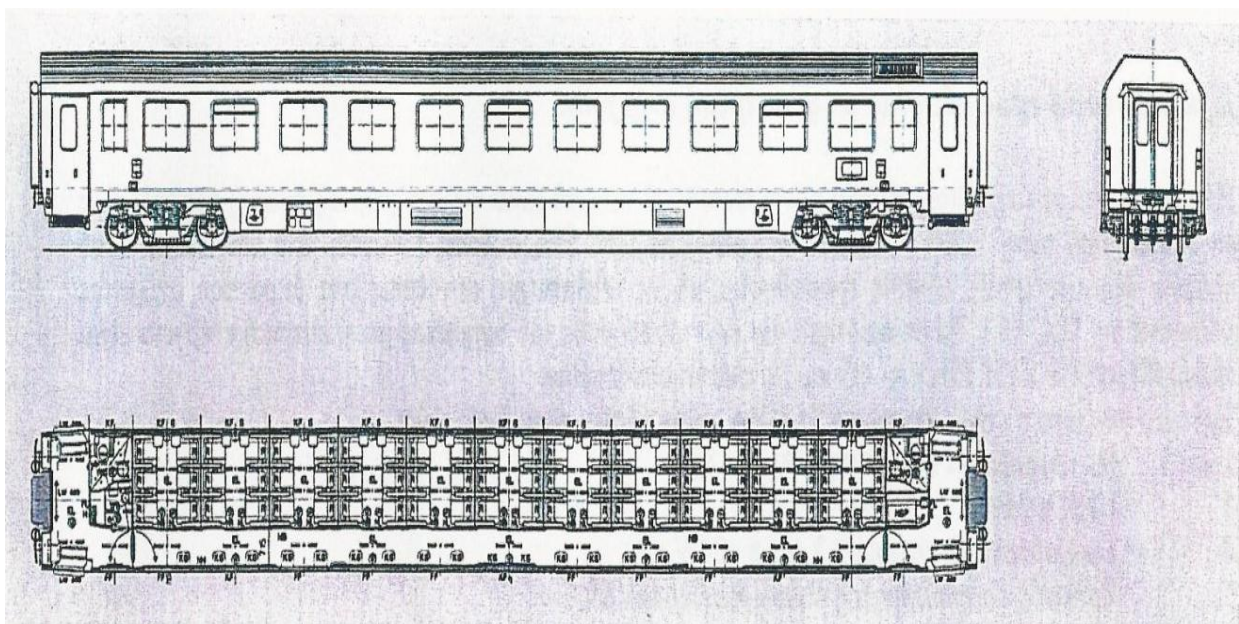


Figure 27 Drawings of BMZ Wagon



Figure 28 Inside of a Wagon

The distance from Thessaloniki to Eidomeni is almost 75 km. The control procedures take place inside rail cars en route and at the end in Eidomeni train station. Checks are carried out by the police and customs authorities. The first stage procedures start from the train station of Kilikis and at the end in Eidomeni station. State authorities enter the train and collect passenger passports. These documents are uploaded in a centralised system by typing the data of the traveller into the form of the Schengen Information System. The second stage of control relies on a simplified biometric authentication of the individual to verify that the person is the one that is holding the travel documents.

In the Eidomeni train station, an expert comes from the Hellenic infrastructure manager to check technical reliability of the wagons. After that, the train is ready to enter the FYROM region.

TRAINOSE estimates that procedures last from 20 to 45 minutes. The time depends on how full the train is.

2.9.3 Optional Procedures in freight trains

A freight train that crosses the borders has the potential to carry immigrants. The size of freight trains can consist of up to 40 wagons and a total length of 545 meters and 1250 ton. In passenger trains, passengers and hosts may notify the authorities of the presence of immigrants. In freight trains, only the train driver can notify the authorities about the presence of immigrants. On the Eidomeni – Thessaloniki route rail network, the train engines are the same as those operating in passenger trains. For freight transportation, four types of wagons can be used.

- Open and bulk wagons (Figure 29)

Railway operators use wagons for many categories of bulk transportation like coil, lignite and metals.



Figure 29 Bulk Wagon

- Covered wagons (Figure 30)

These wagons are used for transportation of goods.



Figure 30 Covered Wagon

- Tank wagons (Figure 31)

TRAINOSE use these wagons for oil transfer.



Figure 31 Tank Wagon

- Flat and timber railcars (container wagons, Figure 32)



Figure 32 Container Wagon

Container wagons are widely used because they have the ability to carry intermodal containers. An intermodal container is a large standardized shipping container, designed and built for intermodal freight transport, meaning these containers can be used across different modes of transport – from ship to rail to truck – without unloading and reloading their cargo (Lewandowski, K., 2016).

All of the wagons have the UIC 505-1 specification and they are made of steel. According to UIC specification OSE bulk wagons are ready for international routes. They are also used for transportation of goods.

TRAINOSE has the ability to transfer containers from Greek regions to Greek borders. On Greek borders, TRAINOSE gives the wagon to ZF CARGO, the major railway operator of FYROM. Exchange of wagons takes part in Gevgeli (Figure 33).



Figure 33 Railway map of North Greece

In Eidomeni station, Greek local authorities check the train for illegal immigrants. Checks are undertaken with policemen accompanied with trained dogs. Following this, freight must pass through customs. In customs, two procedures take place. The first one is the Exit Summary Declaration (EXS) and the second one is the Entry Summary Declaration (ENS).

Similar to passenger wagons railway employees do not have the authorization to perform any check of the wagons for immigrants. In case of an immigrant, locomotive drivers must call the police authority.

Covered wagons and containers are sealed in the departure station or in loading facility with a security seal. Security seals are mechanisms used to seal shipping containers in a way that provides tamper evidence and some level of security. Such seals can help to detect theft or contamination, either accidental or deliberate. Security seals are commonly used to secure truck trailers, vessel containers, chemical drums, airline duty-free trolleys and utility meters. Typically, they are considered an inexpensive way of providing tamper evidence of intrusion into sensitive spaces. TRAINOSE employees test if the seals have been broken before a train departs. TRAINOSE uses ISO/PAS 17712 specification of seals.

Consequently, it is difficult for someone to get in the containers, so it is easy for the controllers to spot a broken seal and perform a comprehensive check by opening it upon request of the authorities.

Every wagon or group of wagons is accompanied by a document complying with CIM specifications (Figure 34). The security seals number is written in this CIM document (Figure 35). The CIM document is an internationally standardized freight document issued in rail transport. CIM stands for "Convention Internationale concernant le transport des Marchandises par chemin de fer". The agreement has been in force since 1965, and constitutes the legal basis for the conclusion of freight contracts in international rail goods transport using one freight document.

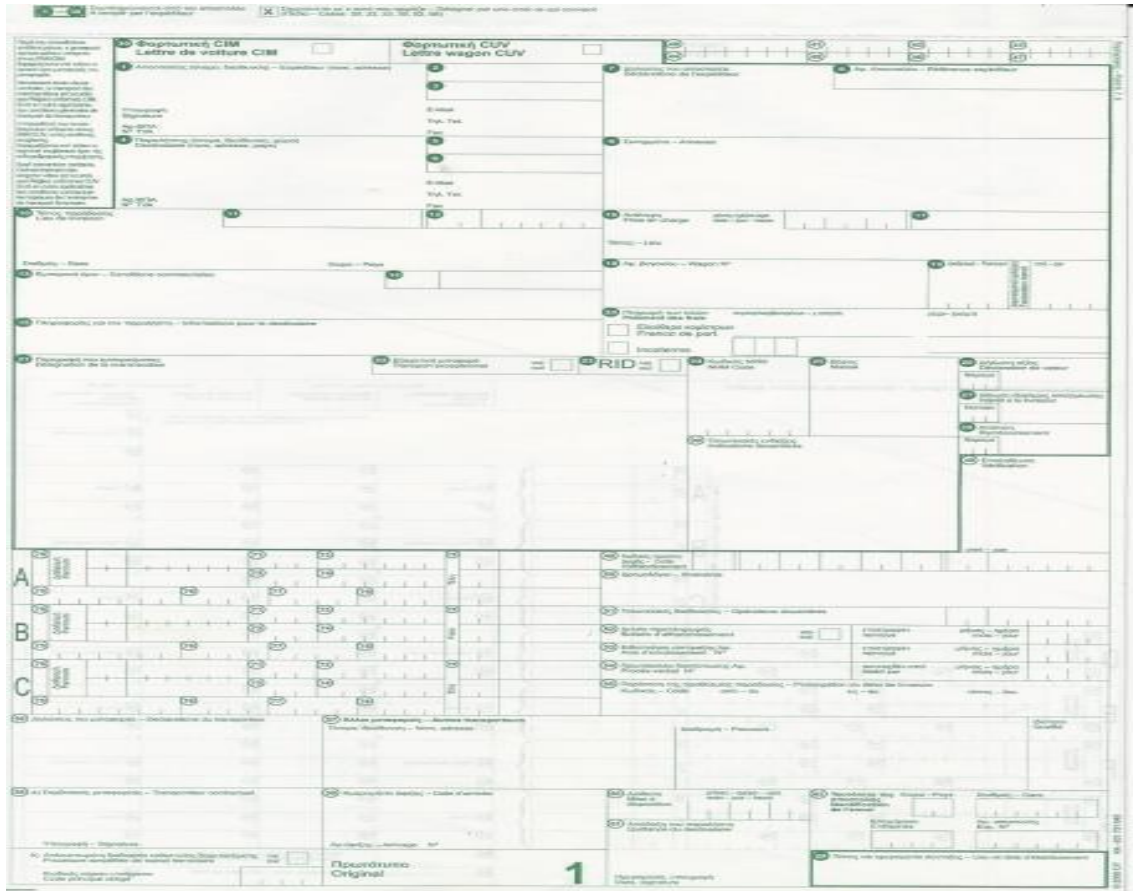


Figure 34 CIM Document



Figure 35 Container Security Seal

After custom and authority's procedures, wagons with locomotive continue towards Gevgeli station. In Gevgeli station the locomotive, driven by TRAINOSE driver, disengages from wagons and returns back to Greek region. From this point on, the local authorities of FYROM are responsible for illegal immigrants.

According to TRAINOSE calculations, the time required to perform checks for the whole train overcomes 45 minutes.

2.10 Key Point summary

It is certain that state borders will exist in the current century and they remain a symbol of state sovereignty. Recent historical and economic events (from 2008 on) started a new Migration Period, similar to the waves in the first AD millennia in Europe. Concerning the legal and illegal migration, it is clear that walls and fences are not able to stop the flow, but can break the waves, winning time for states behind to react; however not for long. The current border management approach, the integrated border management doctrine has to be reviewed and modernized, according to the new challenges. The same applies for technology; current IT systems and equipment -used for border checks- represented advanced technology when they were developed, mostly when preparing for the Schengen Evaluations in year 2007. However, the technology gap is emerging so fast nowadays, being overcome by current situations, that even with regular facelifts and most devoted, well trained personnel, the entire system is becoming obsolete. All end-users are in compliance with Schengen rules and deliver the maximum of their potential; however, there is a clear need on a new integrated border management model and a supporting technical solution.

The iCROSS philosophy is that it is time to introduce a 5th tier in addition to the Four-Tier Access Control. The new tier will be characterized by the cooperation of bona fide travellers and border guards and extensive use of state-of-the art solutions to facilitate border crossing. With this new tier, border checks will start in the country of origin, shortening queues and waiting times at border gates. The solution will not only make the life of travellers easier, but also free up manpower for border guards to cope with illegal migration more effectively.

3 State of the Art Technology Review

Having set out the key features and concepts of border management, a review of the state of the art in each of the technological domains supporting iCROSS is the next essential step. This will inform the requirements analysis in terms of what is currently achievable, what are the shortfalls of current techniques that can be improved upon in the iCROSS solution and what could be achieved when iCROSS is put into practice.

The first step in the methodology is a review of existing border control platforms, in terms of information systems, composed of procedures and data resources, as well as underpinning technologies. This ends with a specific focus on the current practice in iCROSS user groups. The following subsections review the state of the art for each of the contributing iCROSS tools and technologies, including a fitness table (where appropriate) in terms of features contributing to iCROSS requirements. The findings are summarised in a short passage at the end of each section.

The final step is a summary of the contributions of recent substantial related research projects. The combination of information about processes, products and research sets the scene for section 4, User Requirements Capture and Analysis.

3.1 Existing Border Control Platforms Technology review

This section is to provide the review of border control IT solutions used by border guards in their daily work. The focus is put on the platforms used within the European Union and in particular by end users of the iCROSS project. The overall objective is to understand current technological capabilities of border guards and to shortlist European IT systems that can be utilized to facilitate and improve border control process. This section concludes with the description of how the existing solutions can be used in the iCROSS platform and how these solutions can be expanded or improved within the project.

3.1.1 APIS – Advanced Passenger Information System

Advanced Passenger Information (API) or the Advanced Passenger Information System (APIS) relies on providing border authorities and immigration agencies, in particular EU member states, with passengers' data in advance of their arrival to their destination. API data are collected by travel companies (i.e. railway, airlines, maritime) and are shared with proper authorities upon their request. The use of API data has changed over time from being used for purely commercial reasons to helping governments fighting terrorism, crime, smuggling, etc. The transfer of API data was stipulated by the Council Directive 2004/82/EC of 29 April 2004 (Jones).

The data collected under the API requirements include the type and number of travel documents, nationality, full names, data of birth, border crossing point of entry to a particular Member State, code of transport, arrival and departure of the transportation and number of passengers in total as well as the place of embarkation. The implementation of the API Directive has not reached the same level among different Member States. A leading country, with regard to APIS implementation, within the European Union is the United Kingdom. Since April 2015, details from ID cards and passports are gathered at all UK ports and airports while conducting an exit check (Council of European Union, 2004).

3.1.2 PNR – Passenger Name Record

The Passenger Name Record (PNR) is a further extension of the API system. Apart from gathering the same set of information as in API, it assumes the collection of the dates of booking and issuing the tickets, date of travel, name, frequent flyer information, all available contact information (including address, phone number, email), baggage information, travel itinerary, travel status of passenger, and general remarks.

The legislative process of passing the PNR Directive has led to a regulation, which was passed by the EU Parliament and Council on 14 April 2016. The intention of the directive on the use of PNR is to prevent, find, investigate and prosecute terrorist and criminal activities. After the directive is released in the EU Official Journal of the EU, each Member State will have exactly two years to incorporate the new regulation into the national law. Following the implementation of the new directive, airlines with flights between an EU Member State and a Third Country will be required to provide the proper authorities in the EU Member State with the PNR data. The Member State's authorities will not, however, have a direct access to the airline's PNR database. The information will be sent via the "push" method to a single unit, Passenger Information Unit (PIU), of the Member State (Justice and home affairs , 2016).

3.1.3 EES - Entry/Exit System

Entry/Exit System (EES) is a centralised border management system that is expected to be implemented by 2020. This system addresses third-country nationals and their stay duration within Schengen zone. All country crossings for all third-country nationals will be registered by EES. Each entry or exit record will be linked to the traveller's data (identity, biometrics, travel documents). This solution is expected to facilitate the automation of border control process and improve the management of external borders. Moreover, entry and exit records will be used to reduce illegal migration by the detection of overstayers. Currently border guards are in need of such a system due to the fact that the stay duration of any TCN is based on the stamps received in the travel document during entry and exit to/from a Schengen country (European Parliament , 2016).

3.1.4 EURODAC - European Dactyloscopy

European Dactyloscopy, also known as EURODAC, is one of the key systems used by European Union Member States, which is primarily applied to verify the fingerprints of asylum seekers as well as illegal migrants. EURODAC is thus a European fingerprint database, which helps proper authorities to compare the fingerprints of asylum seekers and illegal migrants and to investigate their history of lodging asylum applications. Under current legislation, it is allowed to collect and process fingerprints for asylum applicants as well as illegal migrants who are at the age of 14 or above. According to the Council Regulation No 2725/2000 of 11 December 2000, the specific data, which are stored within EURODAC and then transferred to a particular Member State include the following:

- ten fingerprints,
- the EU country of origin,
- the sex of the person,
- the place and date of the asylum application or the apprehension of the person,
- the reference number,
- the date of fingerprint collection,
- the date on which the data were transmitted to the Central Unit (Council of the European Union , 2000).

The aforementioned regulation further stipulates that the data can be stored through a period of 10 years in case of asylum applicants. The period of time is shortened to the moment of obtaining a citizenship of any EU Member State. In case of illegal migrants, the data are stored for two years. The data can be erased if such a person meets one of the three conditions: 1) he/she is granted a residence permit; 2) he/she no longer stays in the EU territory; 3) he/she is granted the citizenship of any EU Member State (Boehm, 2011).

3.1.5 EUROSUR - European External Border Surveillance System

The European external border surveillance system (EUROSUR) unlike the other described systems and databases, is primarily devoted to the surveillance enhancement of EU external borders. The initial assumption of the system was better protection of the southern borders of the EU with the intent to give a boost to the management of external borders. The main reason for the implementation of the EURO SUR was to improve tracking of illegal migration, detecting trafficking and smuggling of illicit goods and people, as well as prevention of terrorism. In general, the system's functionality is to raise overall situational awareness at the EU boundaries and to enhance the border guard officers ability for operational reaction (Bossong & Carrapico, 2016).

The essential part of EURO SUR is a number of National Coordination Centres (NCCs), which are sited in every Member State. Each NCC manages the surveillance activities and is a centre of data exchange. The collected data are processed by NCC and the relevant information is transferred to other Member States as well as Frontex. Having that knowledge, Frontex generates situational pictures, which provide information on the state of external borders. They are subsequently distributed to Member States through NCCs. Frontex also puts effort in raising awareness of the Member States by supplementing the operational pictures with satellite images and other surveillance devices. The fusion of collected data allows authorities to perform automated vessel tracking, detecting anomalies and predicting vessel positions (Frontex, 2016).

3.1.6 FADO and PRADO - False and Authentic Documents Online and Public Register of Authentic Travel and Identity Documents Online

False and Authentic Documents Online (FADO) is a restricted system for information exchange between document experts. The following data are stored in the FADO database for the purposes of document verification: images of genuine documents, security feature descriptions for each document, images of typical forged and false documents, common forgery technique descriptions and statistics on detected false and falsified documents. A minor part of the document data contained in Expert FADO is released publicly via the Public Register of Authentic travel and identity Documents Online (PRADO) system. Within the PRADO, registered documents are divided into categories (e.g. "Passports", "Identity Cards", "Visa" etc.) and types (e.g. "Ordinary", "Military", "Diplomatic"). Apart from border security applications, PRADO can be utilized by organisations with a need or legal obligation to check identities (e.g. bank institutions, vehicle rental companies) (EUR-Lex, 2016) (Council of the European Union, 2016).

3.1.7 Interpol FIND

Interpol FIND (Fixed INTERPOL Network Database) and MIND (Mobile INTERPOL Network Database) are integrated technical solutions for front-line law enforcement agencies (e.g. border police). They were created to provide the front-line officers with reliable, accurate and up-to-date

information. The purpose of these solutions is to facilitate searches of people, vehicles and documents at international transits.

3.1.8 SIS II – Schengen Information System II

Schengen Information System II is a database used by European countries, which constitutes the pillar of border checks performed within EU. It has been created in order to support external border control and law enforcement cooperation in Schengen States. Competent authorities are enabled to enter alerts that are stored in the database. Information about wanted or missing persons or objects can be incorporated within the alerts. Moreover, it includes instructions on what to do when such a person has been found. As noted by the European Commission, the main purpose of SIS II is to help to preserve the internal security in the Schengen States in the absence of internal border-checks (Migration and Home Affairs, 2015).

SIS II includes three major components, i.e. the central system, national systems and the communication network. The first component is a central system, which is responsible for data storage in itself and transfer of it to national parts of the system through a secure network. The alerts, which are created in the national parts of system are transferred to the central part of system in real time. A national system could contain a synchronised copy of the main system. SIS II is a highly secured system, it is only accessible by authorised users within competent authorities (e.g. national border control, police). The EUROPOL and EUROJUST users have special rights to carry out particular types of queries on specified alert categories (Migration and Home Affairs, 2015).

Each member state operating the system needs to set up the national SIRENE Bureau. The SIRENE Bureaux should be operational 24/7 and it is responsible for:

- Providing information on alerts,
- Validating alerts of wanted persons,
- Supervising the quality of data and compatibility of alerts,
- Coordinating activities of alerts related to SIS,
- Handling requests to access personal data,
- Contacting the state that issued the alert when the required action cannot be taken (Brouwer, 2008).

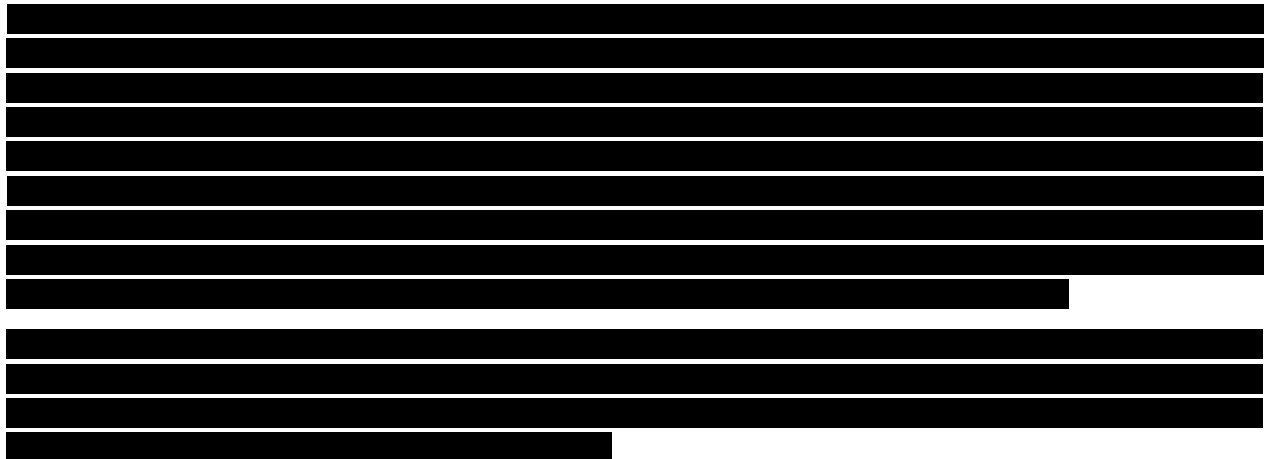
3.1.9 VIS – Visa Information System

Visa information System is an EU database comprising information on visa applications lodged by Third Country Nationals (TCN), who require a visa to enter the Schengen area. The system was established in June 2004. VIS is built from two layers, the first being a central IT system and the second being communication infrastructure. The communication infrastructure links the central European system to national systems. VIS has been created, inter alia, in order to facilitate checks and issuance of visas. The other purposes of VIS, which are listed by European Commission, include: fighting abuses, protecting travellers, and enhancing security. These objectives are achieved, for example, by a utilization of biometric data for visa holder identification (Blazacq & Carrera, 2005).

The biometric data, required from persons applying for a visa, includes 10 fingerprints and a digital photograph. Moreover, individuals applying for a visa for the first time must apply in person in order to register the aforementioned mandatory biometric features. For future applications, biometric data stored in the central VIS database can be used. Regarding the storage time of collected data, it is limited to five years under current regulations (Migration and Home Affairs, 2015).

The data are stored in a secured central database. In order to maintain security, the access to VIS database is granted only to the authorities responsible for performing checks at external borders and within the national territories. Moreover, in exceptional cases, VIS database can be accessed by the law enforcement authorities for crime or terrorism prevention issues (Migration and Home Affairs, 2015).

3.2 Document Authenticity Analytics Tools



In this section, a survey regarding state of the art Document Authenticity Tools, being commercially available is presented. Several technologies and methodologies which are used for the authenticity verification of documents are depicted through the comprehensive description of existing products' features. Consequently, this technology review will reveal all gaps and limitations inherent in the state of the art solutions that are currently used and will contribute in the design improvement and better implementation of the iCROSS DAAT tool.

3.2.1 Document authenticity verification device Regula 4205D

The Regula 4205D device is intended for advanced authenticity verification of passports, ID cards, travel documents, visa stamps, seals, driving licenses, vehicle registration certificates, banknotes, revenue, securities and other documents with security features. The Regula 4205D is equipped with modules for reading MRZ and RFID chips and has an integrated information reference system to compare the examined document with the document template from the database.

The device supports capturing images using white, infrared, ultraviolet and coaxial lights. Optionally it can be equipped with a module for reading smart cards. The device is supplied with software development kit (SDK) for integration into existing end-user systems.

Possible applications of the device include: border control services, aviation security services, law-enforcement agencies, immigration services, financial institutions, hotels, car rental and leasing companies, cellular companies, business centers security service, event-agencies and medical institutions (Regulaforensics.com, 2016).

3.2.2 Coesys Document Verification

Coesys Document Verification is a distributed software system that verifies the electronic and physical security features of identity documents. Passports, visas, ID cards, driver's licenses and

many other identity documents can be checked against templates that are stored in a database, administered centrally and automatically synchronized into local repositories. As part of the Coesys Border and Visa Management suite, Coesys Document Verification can be deployed together with a biometric identification solution to determine whether the document bearer is the rightful owner. Coesys Document Verification also claims to address the needs of the private sector (telecoms, currency exchange, money transfer, post offices, car rental companies and more). It can be delivered as a standalone application or a software development kit (SDK) that integrates into a proprietary or third-party system (Gemalto.com, 2016).

3.2.3 Keesing ID AuthentiScan PREMIUM

AuthentiScan PREMIUM is an automated solution for extensive ID document authentication. This solution offers broad-based verification and performs approximately 40 automated checks on a document. It supports scanning, inspecting and storage (optional) of many national and international ID documents. This PREMIUM solution offers broad-based authentication and determines whether a document is genuine or counterfeit. Checking ID documents using AuthentiScan procedure requires placing the document on the passport reader and the system automatically performs the necessary checks. AuthentiScan is powered by Keesing Documentchecker Database, and as a result there is a possibility to perform additional checks by comparing a document to reference material retrieved from a reference database for ID documents. This database covers passports, driving licenses, ID cards and visas from over 200 countries and organisations (Keesingtechnologies.com, 2016).

3.2.4 Identity Document and E-Passport Scanner (PRMc)

The Identity Document and E-Passport Scanner by ATH Hungary is a multi-purpose scanner that provides automatic, accurate data extraction and verification with the ability to read multiple types of identity documents: passports, e-passports, ID cards, visas and driver licenses. The printed data is extracted from the entire page (MRZ, VIZ and 1D & 2D bar codes) while digital data is obtained from contactless (RFID) and contact smart chips. The standard and enhanced versions of the scanner both possess multiple illumination sources (visible white, infrared images (IR) and ultraviolet (UV)), hardware-assisted reflection removal (RR) and the optional OVD visualization function. The PRMc scanner is suitable for several applications including border control and immigration and security and commercial environments such as banks, hotels and telecom retailers (Arh.hu, 2016).

3.2.5 RealPass-V

RealPass-V is a full page optical and RFID Passport reader, offering automatic document detection, single-step reading, tunable RFID antenna and a lay-on type scanning. The device processes optical and graphic data from data page, and reads RF chips with ICAO standard security protocols. Using a Single-Step Reading Technique, RealPass-V claims that it takes less than one second to capture and display a page with light and infrared imaging. Moreover, it is equipped with UV & IR illumination features to support high-security applications. Under UV illumination light, invisible security threads in various colors appear that are not visible in normal lighting conditions (Supremainc.com, 2016).

3.2.6 DERMALOG VF1

The Dermalog VF1 is a solution for national registration and automated border control suited for integration into eGates. The DERMALOG VF1 is a multi- purpose scanner able to capture fingerprint

and passport images on the same scanning surface. The VF1 has the additional capability to capture signatures on the scanning area. Additionally, the scanner can detect fake fingerprints in order to prevent fraud and misuse (Dermalog.com, 2016).

3.2.7 OCR640e Desktop Full-page Document Imager

The OCR640e Desktop is a full-page multi-illumination ePassport reader. It captures UV and IR, as well the full page of a passport in color. The reader also decodes the machine readable zone (MRZ) and processes RFID data – including the holder's image – from the chip. The OCR640e is also able to compensate for out-of-position MRZ data, so the advanced recognition engine claims to provide accurate and fast document reading capability, allowing large volumes of documents and smart cards to be processed quickly and efficiently. The unit features blue, amber, green and red LED lights to keep the user informed of statuses from *ready to scan through* to *processing and successful scan*, or that there is *an issue with the document*. A programmable audio beep provides additional user feedback to confirm successful scans (Access-is.com).

3.2.8 MBMS - Multi Border Management System

MBMS (Multi Border Management System) is a border management system developed by Semlex to reinforce the efficiency and productivity of security officers. Its technology facilitates verifications and accelerates the border crossing procedures. Among other services the MBMS system claims to offer verification of travellers' identity and documents, recording of border crossings in a centralized database, quick and reliable processing of information, recording of entries and exits, establishment of automatic crossing gates (e-Gates) and connection to international databases (24/7 Interpol, ICAO) (Semlex.com, 2016).

3.2.9 VISOTEC Expert 600

VISOTEC Expert 600 is a document reading and verification device along with the corresponding software (VISOCORE Inspect and VISOCORE Verify) for enhanced security. The VISOTEC Expert 600 reads different document types which correspond to the standards issued by the International Civil Aviation Organization (ICAO), including ID cards, passports and visas. The device checks visual security features under different lighting as well as integrated security chips, no matter where the chip is located in the document. This high-end document reading and verification device can also handle extra-thick or stapled passports. A special advantage of the VISOTEC Expert 600 is that it has been certified by the German Federal Office for Information Security (BSI) in accordance with its technical guidelines. The system built-in variant can be easily integrated into eGates and check-in, ticket or cash machines (Veridos.com, 2016).

3.2.10 P1000

P1000 is a compact Identification Document reader. It captures full color or greyscale images of all travel documents including non-ICAO passports. P1000 is applicable to travel agencies, car rental, kiosks, hotel check-in, banking, finance and border control (Iris.com, 2016).

3.2.11 B5000

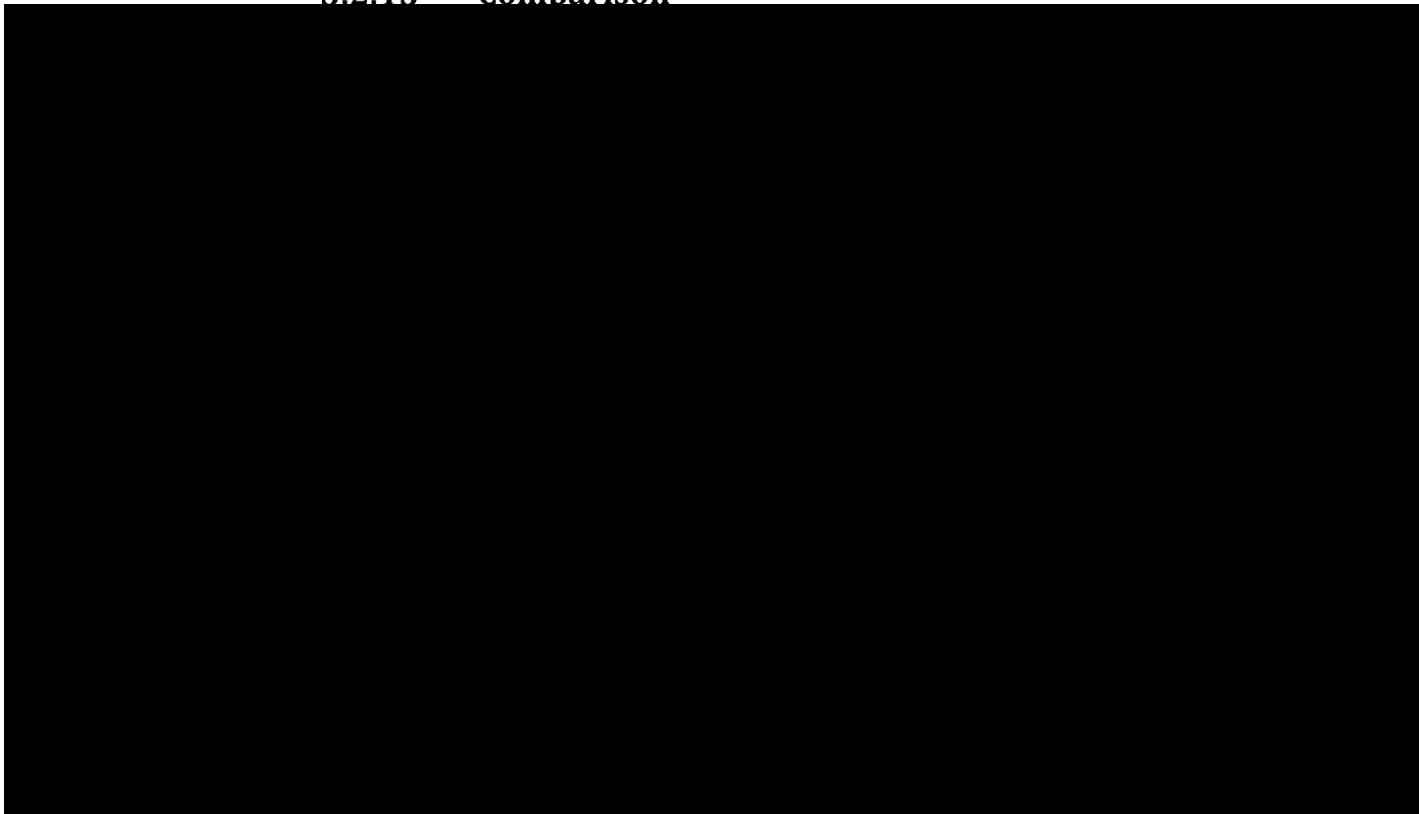
B5000 automatically authenticates documents that are used as proof of a person's identity. This full page document reader captures images using visible, coaxial, infrared and ultraviolet light sources to perform multiple security checks, ensuring the ID being presented is valid. More specifically, the B5000, as a combined hardware and software solution, claims to read and authenticate

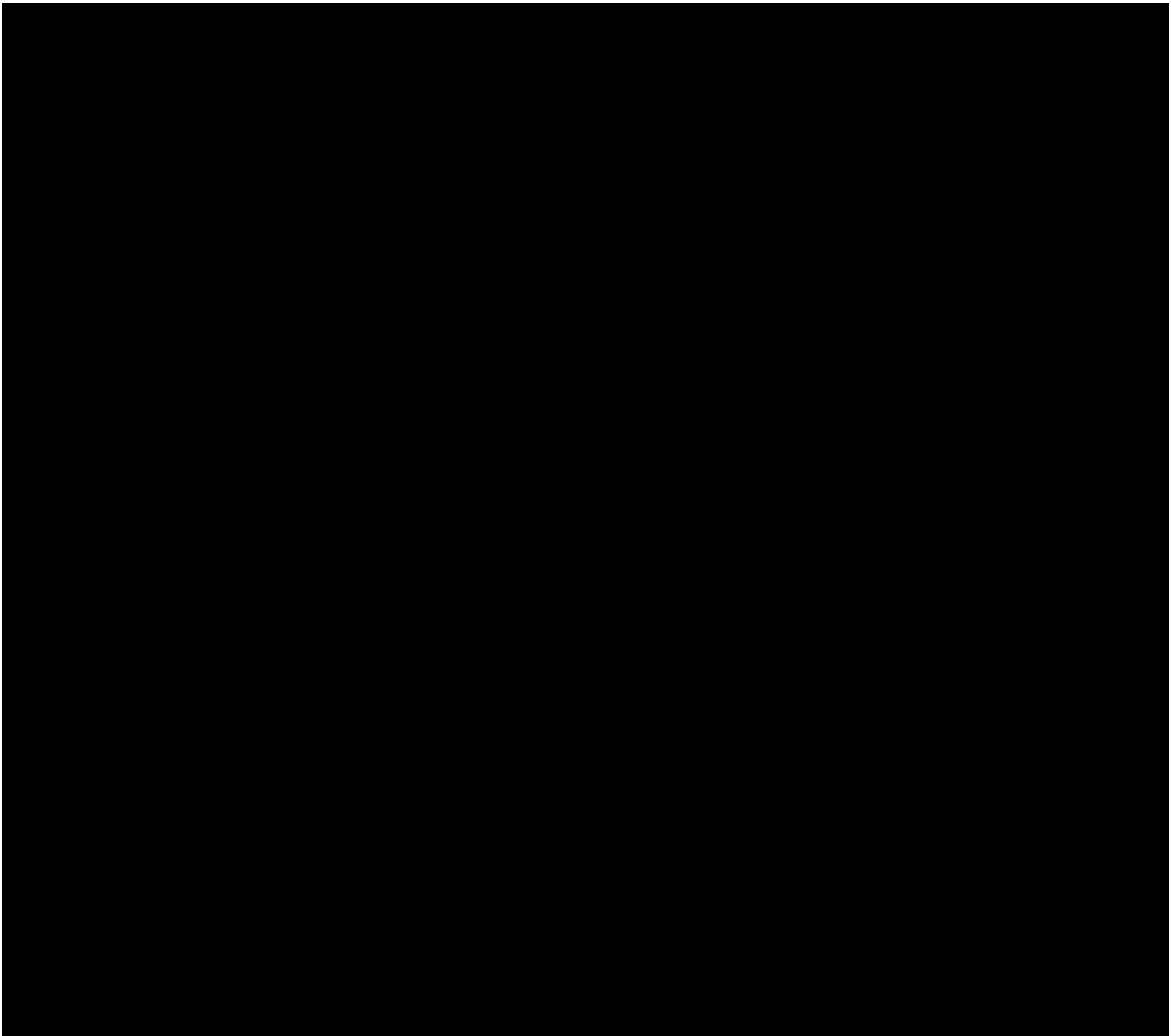
international travel and identity documents in only a few seconds. Moreover, it authenticates covert & overt security features helping identify forgeries using the Documetrics database, meets each country-specific privacy and data protection laws and is suitable for desktops, booths and kiosks. The B5000 can be deployed in a variety of situations such as border control, police identity checks, court attendance, healthcare and welfare program enrolment (Morpho.com, 2016).

3.2.12 System and Method for Automatic Document Verification – Patent US 20020145747 A1

The proposed system for verifying a printed document is implemented to automatically compare first and second images and provide an output with respect thereto. In an illustrative embodiment, the inventive system includes a computer for providing a first electronic image of a document. The image may be provided via a network such as the Internet. A printer is coupled to the computer and driven to print the document. The document is then scanned to provide a second electronic image of the document. The scanned image is then compared to the original image to provide verification of the printed output. For text based documents, the first and second images may be converted to text using conventional optical character recognition software to facilitate comparison. Additionally, a mechanism is provided to detect a file characterization by which a restriction may be imposed on the number of the documents to be printed. If a document is restricted, successful printouts above the restriction are disabled. As a further refinement, a second mechanism is included to enable a fingerprint to be printed on the restricted document. When scanned, the fingerprint provides an indication of the operability of the printer and the scanner. In the event the fingerprint is not detected, the printer is disabled. This mechanism would be useful in a pay-to-print application to frustrate fraudulent efforts to disable the scanner and thereby cause the printer to output unauthorized printouts (Burquist, & Boockholdt, 2001).

3.2.13 Comparison





3.2.14 Summary



According to these findings, it is necessary to develop a tool that will consider both the users' requirements and all interdependencies of the features that other devices offer. Therefore, the aim in this section is to determine the specifications for the development of the DAAT tool to improve the comprehension of the requirements. iCROSS aims to overcome any ethical issues, and pass through the legal framework supporting the effectiveness of EU border control. It will also apply these tools and knowhow and expand its purpose for the differing requirements and needs that arise for document processing. Particularly in terms of their authenticity during border control operations by providing a full ICT customized and automated solution, in real-time and during the border control operations.

3.3 Automatic Deception Detection System (ADDS)

Human interest in detecting deception has a long history. The earliest records date back to the Hindu Dharmasastra of Gautama, (900 – 600 BC) and the philosopher Diogenes (412 – 323 BC) according to Trovillo (1939). Some quite barbaric physiological tests for lying were devised (applying the tongue to a red hot iron is believed to be based on the idea that a liar with a dry mouth would burn sooner), other methods included measuring the pulse and early attempts to measure blood pressure (Trovillo 1939). Angelo Mosso invented various techniques and instruments in the late 19th and early 20th centuries using pulse and blood pressure to investigate deception and emotional states. Following this, the Polygraph (International League of Polygraph Examiners, 2016) was invented, by John Augustus Larson in 1921, to detect lies by measuring physiological changes related to stress. This has been followed by other techniques such as voice stress analysis. Newer techniques have been proposed using techniques such as EEG or fMRI to measure changes in brain activity indicating deception.

3.3.1 The Polygraph

The Polygraph is a recording instrument, which displays physiological changes such as pulse rate, blood pressure, and respiration, in a form where they can be interpreted by a trained examiner as indicating truthful or deceptive behaviour. Additional sensors have been added recently including measuring Galvanic Skin Resistance and sensors to attempt to detect countermeasures intended to deceive the test. Currently respiration is measured by a pneumograph wrapped around the interviewee's chest, blood pressure and pulse are measured by a blood pressure cuff attached to the arm or plethysmograph attached to the finger (Lafayette, 2016). A polygraph test takes a minimum of 1.5 hours but can take up to four hours depending on the issue being tested for (Lie Detectors UK, 2016). Wiring up a person to a polygraph is also an intrusive process. Lafayette and CSS offer wireless polygraph sensors (Wireless Lie Detector Polygraph, 2016), however, these require the same sensors to be attached to the body, as well as wireless transmitters and simply remove the cable from the sensor to the polygraph itself (Figure 36).



Figure 36 The Polygraph

Individual scientific studies can be found which support (Mangan et al, 2008) or deny (Honts & Revy, 2015) the validity of the Polygraph. A meta-study (Saxe et al., 1985) conducted in 1985 found 10 studies from a pool of 250 were sufficiently rigorous to be included. From these they concluded that under very narrow conditions the Controlled Question Test (CQT - the standard Polygraph test which could be used at border crossings) could perform significantly better than chance, but these results would still contain substantial numbers of false positive, false negative and inconclusive classifications. They also stated that many conditions needed to achieve this may be beyond the control of the examiner. Constructing a good set of control questions for this test requires substantial information about the interviewee's background, occupation, work record, criminal record to be collected before the exam.

Another form of Polygraph test, the Concealed Knowledge Test (CKT, also known as Guilty Knowledge Test) is acknowledged as having some effectiveness by critics of the CQT (Meijer et al. 2016). This is not a lie detection test, but a test of whether a suspect has information related to a crime that an innocent person would not possess. It involves presenting information and testing for a stress reaction. This technique requires carefully crafted interviews for each individual questioned about a crime. Polygraph prices are not widely published, but industry sources suggest a cost of about £5,000 for a typical configuration.

The Polygraph is used in the UK with sex offenders for maintenance testing (Grubin, 2008) - preventing offenders released from prison on license from re-offending. However, the main value of the Polygraph appears to be a broker between an offender who genuinely wishes to change his behaviour and the probation officer, in one study (Kokish et al., 2005) 5% of the offenders reported that they had falsely admitted to things they had not done to comply with incorrect polygraph assessments.

3.3.2 Functional Magnetic Resonance Imaging (fMRI) detection

Functional Magnetic Resonance Imaging (fMRI) is a technique that measures changes in activity of areas of the brain indirectly by measuring blood flow (which changes to supply more oxygen to active areas of the brain). It has been proposed that there are reliable relationships between patterns of brain activation and deception that can be measured by fMRI. It has also been reported that although fMRI is seen as overcoming some weaknesses of the Polygraph, for example by having

an explanatory model based on cognitive load (Meijer et al., 2016) it is highly vulnerable to countermeasures (in common with EEG-based approaches).



Figure 37 Philips MRI Scanner

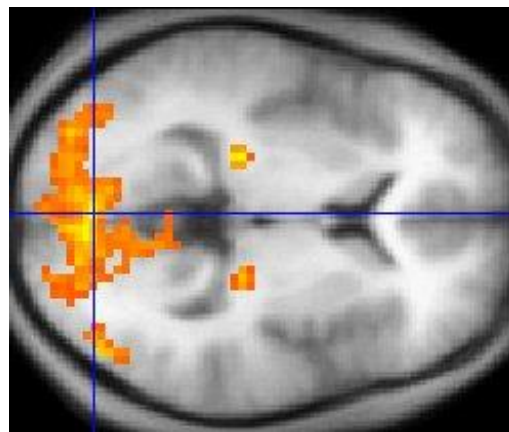


Figure 38 fMRI Scanner

A metastudy (Farah et al., 2014) of 23 published studies of fMRI lie detection found that reliable patterns of activation did exist, but that other psychological processes may be confounded with deception in many tasks causing observed fMRI effects that were incorrectly attributed to deception.

Nevertheless, a franchise-style organisation, No Lie MRI Inc. offers opportunities to set up fMRI lie detection centres. The specified requirements are for a 3 Tesla MRI scanner (No Lie MRI. 2006.), costing about \$3M, weighing 13 tons and requiring a specially constructed room of a minimum of 33 square metres floor space and 3-phase power supply (Siemens Healthcare Limited. 2016.).

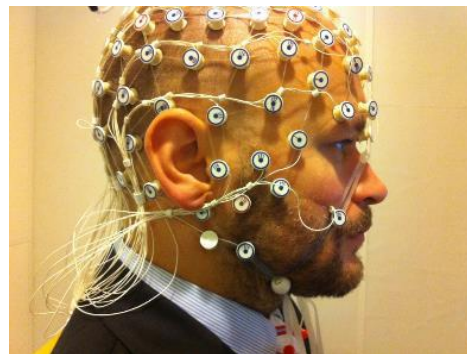


Figure 39 EEG Electrode Placement

3.3.3 Electroencephalogram (EEG) detection

EEG is a technique that measures changes in the electrical activity of the brain, through electrodes attached to the scalp (NHS. 2015.). A clinical EEG test takes 20- 40 minutes. Conductive gel is applied to the scalp before the test and is cleaned off after the electrodes are removed. Fairly complex pre-conditions in terms of washing hair, food consumption, recording medical history and sleep are required for clinically useful EEG results. Also, the test must be administered by a technician who has completed an accredited electroneurodiagnostic technology training program (Study.com. 2016). A clinical EEG test typically costs between \$200 and \$700 (Costhelper Inc. 2016) and the capital cost of a typical basic EEG system (EEG LTM & PSG Systems & Accessories) costs \$ 5,995.00 (MFI Medical. 2016), but only has a 90-day warranty. The combined electrical signals are referred to as brainwaves and some, Event Related Potentials have distinct signatures and occur after certain stimulus events (Wolpe et al., 2005).

The P300 is an ERP which is believed to be associated with evaluating a stimulus or categorizing stimuli. The P300 has been proposed a suitable measure for the CKT and it is accepted in Japanese courts (Rosenfield et al., 2013). There is no current use for it in conventional (CQT) lie detection. Although there is evidence that that, like fMRI, EEG is vulnerable to spoofing (Meijer et al., 2016), constructing more complex CKT tests may restore accuracy to around 90% (Rosenfield et al., 2013).

3.3.4 Voice Stress Analysis

Voice Stress Analysis (VSA) is a technique that analyses physical properties of a speech signal as opposed to the semantic content. The technique is fundamentally based on the idea that a deceiver is under stress when telling a lie and that the pitch of the voice is affected by stress. More specifically, the claim that micro tremors, small frequency modulations in the human voice, are produced by the automatic, or involuntary nervous system when an interviewee is lying. There have also been claims that the increased cognitive load of deception creates micro tremors (Walczyk et al., 2013).

The weight of scientific analysis is that, whatever the assumed underlying model, VSA performs no better than chance and has been described as “charlatanry” (Eriksson & Lacerda, 2007). Although the position remains the same currently (Levitan et al., 2015 individual differences ref), voice stress has been occasionally repackaged by commercial companies. One such example is Layered Voice Analysis (LVA). LVA produced by Nemesysco (Israel) claims to apply 8,000 mathematical algorithms to 129 voice frequencies which are indicators of the reactions to the stress of telling lies. Several studies have reported LVA to be ineffective (Horvath et al. 2013). Horvath’s own findings will not be discussed here because he used Polygraph interviews to determine “ground truth” for his recordings. No pricing information is published by Nemesysco, however in 2009, the Guardian newspaper published a report that the UK government had spent £2.4M on a trial of the Nemesysco system and that DWP statisticians concluded that the VRA system did no better than flipping a coin (Arthur, Charles. 2009).

3.3.5 Speech analysis

The most recent work in this area is contained in the INTERSPEECH 2016 Computational Paralinguistics Challenge: Deception, Sincerity & Native Language. Inspection of a sample of responses to the 2016 challenge shows them to be either paralinguistic, phonemic or a combination of the two, e.g. the Low Level Descriptors such as psychoacoustic spectral sharpness (Levitan et al. 2016) or phonetic features such as phonemes (Herms, 2016). These techniques achieved approximately 67% using a technique called “Unweighted Average Recall” intended to take account

of the fact that the Deceptive Speech Database (DSD) (dataset) from the University of Arizona was unbalanced (test set contained 24% deceptive / 76% truthful classes). We have not found evidence of a significant degree of paralinguistic research outside English.



Figure 40 Analysis of Text

Semantic Analysis techniques examine the words used by an interviewee and their meanings. Verbal content analysis focuses more on the meanings of the utterances made than the manner in which they are said. There are three prominent techniques (Bogaard et al., 2016): Scientific Content Analysis (SCAN) developed by a former Polygraph examiner from professional experience, Criteria-Based Content Analysis (CBCA) developed by psychologists for evaluating children's testimonies in cases of alleged sexual abuse and Reality Monitoring (RM) developed by memory researchers for determining whether a memory was genuine or false. Bogaard et al. (2016) reported that metastudies provide accuracy figures of around 70% for CBCA and RM.

A typical example is CBCA (Welle et al., 2016), which uses a 19 point scoring checklist to evaluate the credibility of a child's statement in sexual abuse cases. Three categories are checked: General (e.g. the logical structure), Specific Contents (e.g. descriptions of interactions) and Motivation-related Contents (e.g. admitted lack of memory). Witness statements are recorded, manually transcribed (verbatim) and anonymised. They are then scored by expert CBCA raters (e.g. trained psychologists / psychiatrists). Each item on the checklist is scored 0 (absent), 1 (present) or 2 (strong) and the scores totalled. The expert then uses the score to make a judgment on the credibility of the statement. In (Welle et al., 2016) the experts were advised that a score (out of 38) below 10 increased the likelihood of a false statement whereas a score greater than 16 was more representative of a credible statement. Welle's study found an inter-rater agreement of 0.74 and an average overall accuracy of 75%, although it performed well on true positive cases, the technique scored lower than chance on true negatives. They also reported that several other studies showed SCAN could not discriminate between truthful and deceptive statements.

3.3.6 Facial Microexpressions

Facial Microexpressions are short-lived, unexpected expressions. There is said to be a small "universal" set of expressions of extreme emotion: disgust, anger, fear, sadness, happiness, surprise, and contempt, meaning they are common across cultures. A formalised method of encoding micro expressions was defined by Paul Ekman, who developed commercial tools for training interviewers to recognise them (Ekman, P., 2016). One of the resources is a manual on a Facial Action Coding System for training in expression recognition. This has generated a large body of research in automating FACS for applications such as lie detection. There are also a number of

patented techniques for automatic FACS e.g. by Apple. However, in practice, the vast majority of published research consists of papers which make a brief assumption of the techniques importance to lie detection and then simply introduce a new image processing algorithm (or algorithm variant) designed to recognise such expressions when they occur, e.g. see (Su-Jing Wang et al.2014).



Figure 41 Universal Facial Expressions of Emotion

Much of this research is built on flawed methodology. In particular using datasets based on highly artificial “posed” images using actors or students provided with highly specific instructions (Savran et al., 2008; Yin et al., 2008) or even training in how to produce facial actions (Bartlett et al., 1999, Porter et al., 2012), low numbers of detectable Ekman micro-expressions in spontaneous interviews (Valstar et al., 2012) and a low Classification Accuracy (CA) for those micro-expressions actually found (Valstar et al., 2012). In 2009, the York dataset was published. This consisted of video recordings of participants either lying or telling the truth about the content of unemotional (Hawaiian landscapes) or emotional (footage of surgical operations) video clips while they viewed them (Warren et al., 2009). The experiment also recorded a baseline truthful account of the participants describing their hobbies. Human judges were trained in two of the Ekman techniques and asked to classify the emotional and unemotional recordings. The study found that the judges performed better than chance on the emotional recording, but were worse than chance on the unemotional recordings.

Recent attempts to produce improved databases have had mixed success. The two most prominent: The Spontaneous Micro-expression Database (SMIC) (Xiaobai Li et al.2013). and Chinese Academy of Sciences Micro-expression II database (CASME II) (Yan et al., 2014) followed the York set in recording the participants watching highly emotional video clips (e.g. beating a pregnant woman), but focused on suppressing expressions rather than lying about them.

The CASME II study reported difficulties in labelling the microexpressions and the constrained laboratory conditions for the experiment. The maximum accuracy for the automated detection system was 63.41%. The SMIC study found that 25% of the participants in the study showed now microexpressions at all (in 35 minutes of video) and the others showed between 2 and 39 microexpressions. The maximum accuracy for their automated detection system was 65.5% (against a chance level of 50%).

Virtually all of the findings from microexpression studies are closer to a CKT than genuine lie detection, so they do not constitute persuasive evidence for using the technique at border crossings. The single exception we have found (Su & Levine 2016) largely uses the technique disclosed in the Silent Talker patent, with the exception that the initial feature detection and channel encoding is

done using Ekman FAUs to detect blinks etc. Consequently, there would be very serious obstacles to commercialisation of their technique.

3.3.7 Silent Talker

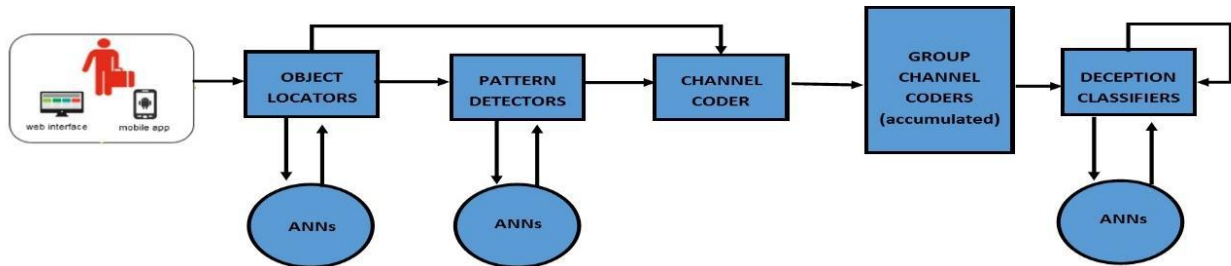


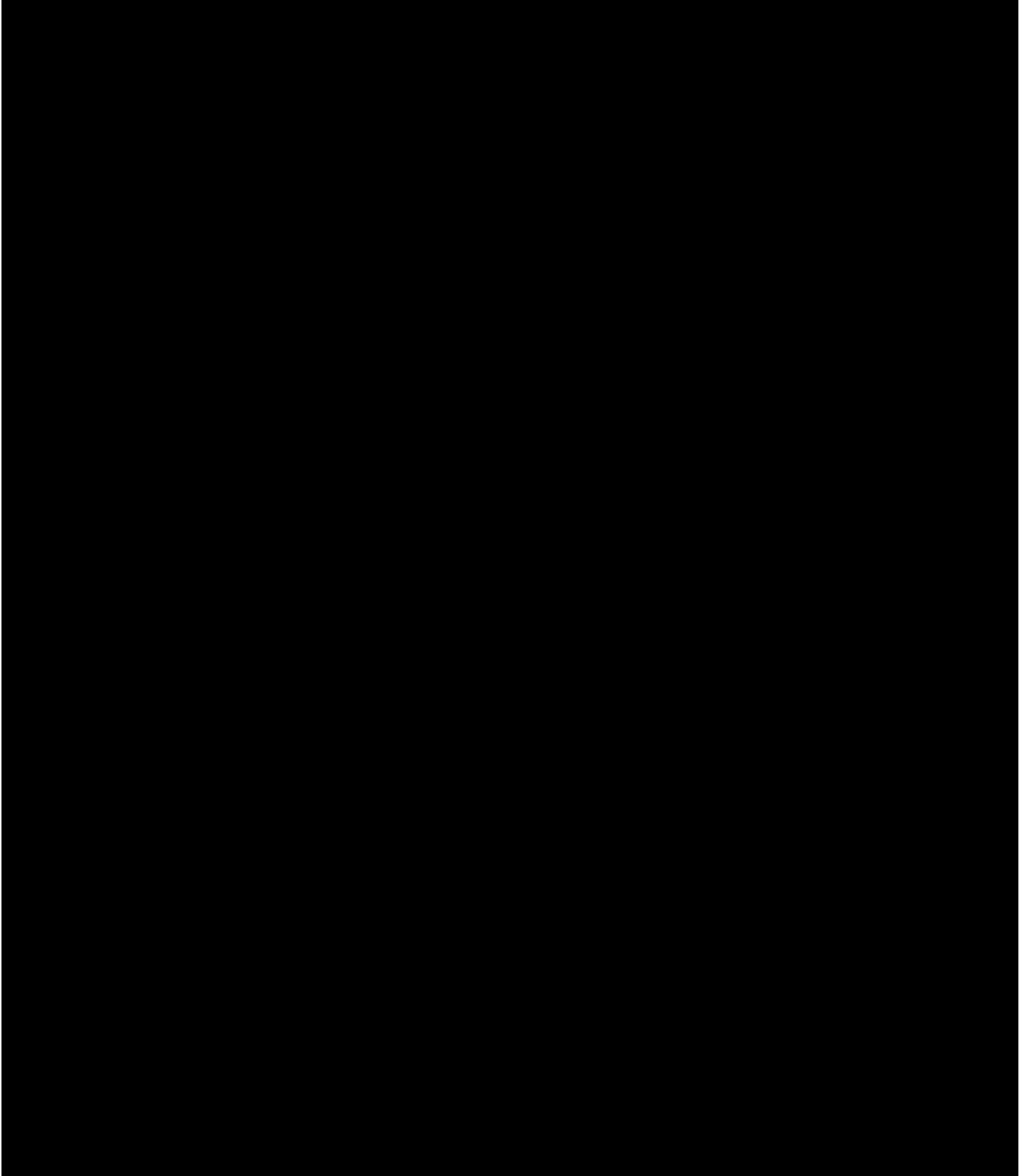
Figure 42 Silent Talker Architecture

Silent Talker (Figure 42 Silent Talker Architecture) is an invention that uses complex interactions between multiple channels of microgestures over time to determine an internal mental state, in particular that of a deceiver. A microgesture is detected by locating a suitable object (e.g. an eye), detecting information about its state (pattern detectors – e.g. eye fully-open) then encoding this in a channel (e.g. fully-open to half-open to closed indicating a wink or blink) over a time interval (e.g. 3 seconds). Microgestures are significantly different from microexpressions, because they much more fine-grained and require no functional psychological model of why the behaviour has taken place.

Silent Talker (ST) was designed to answer the criticisms of the psychology community that there are no meaningful single non-verbal indicators of deception (such as averted gaze), by combining information from many (typically 40) fine-grained nonverbal channels simultaneously and learning (through Artificial Neural Networks) to generalise about deceptive NVB from examples. In this respect it does not depend on an underlying explanatory model in the same way as other lie detectors. However, it does have a conceptual model of NVB. This model assumes that certain mental states associated with deceptive behaviour will drive an interviewee's NVB when deceiving. These include Stress or Anxiety, Cognitive Load, Behavioural Control and Duping Delight. Stress and Anxiety are highly related, if not identical states. Associated non-verbal behaviours include hand gesture time, nodding frequency and nodding time (Feiler & Powell, 2015). In a lie detection experiment focused on Cognitive Load, Vrij et AL (2000) reported significant differences between liars and truth-tellers, with liars making fewer illustrators gestures and more hand and finger movements. In a study of liars showing signs of deceit as a result of experiencing emotions or cognitive load or because they attempt to appear convincing, Caso et al. (2005) reported that attempted control was the dominating factor and that participants exhibited more pauses, fewer eye blinks, and (male suspects) fewer hand and arm movements when they lied. Duping Delight was proposed by Paul Ekman as an emotional driver arising from exhilaration, glee or pleasure of successful deception (Ekman, 1981). Duping delight could result in increasing limb movements or frequency of smiles (Lawson et al., 2013).

They key feature of ST as a machine learning system is that it does not matter whether particular psychologists are correct about particular NVB gestures, ST was given a set of candidate features and worked out for itself which interactions over time indicated lying. Evidence to date is that no individual feature can be identified as a good indicator, only ensembles of features over a time interval provide effective classification. Early experiments with ST showed classification rates of between 74% and 87% ($p < 0.001$) depending on the experimental condition (Rothwell et al., 2006).

3.3.8 Summary of State-of-the-Art Deception Detection Systems



research is equivocal this claim. *Analysis of Context* indicates that substantial analysis of a case is required to design an interview before using the Polygraph or Stylometric techniques. *Baseline-free* indicates that Polygraph and Voice Stress techniques require a baseline of truthful behaviour to be recorded before the interview to measure potentially deceptive behaviour against. *Training costs* shows that Polygraph examiner, clinical or psychological skills are required for an interviewer for all techniques except Voice Stress, Automatic Microexpressions and ST. *Setup time* shows that all of techniques except Voice Stress, Automatic Microexpressions and ST require a substantial preparation time with the interviewee before the interview can start (e.g. taking medical history, applying electrodes, sensors, briefing interviewee etc.). *Execution time* indicates that Polygraph, Stylometric and offline Microexpressions take a substantial time to conduct the test. *Real time* shows that all of the techniques except Stylometric and offline Microexpressions provide some real-time information about the interviewee behaving deceptively. *Accuracy* shows that fMRI, Voice Stress and offline Microexpressions have a body of scientific reviews that suggests they are not sufficiently accurate for iCROSS. Opinions on the Polygraph's accuracy are highly polarised. EEG is too vulnerable to countermeasures to be accurate for general lie detection. Automatic Microexpressions have a single experimental study to support accurate classification, ST has been peer reviewed in one established Psychology Journal and one established AI journal, but the Fathom comprehension technique derived from ST has also been published in peer-reviewed medical conferences. iCROSS will provide an opportunity for further validation of the ST methodology. *General population* shows that there are many medical conditions that prevent the use of fMRI and that there is a proportion of the population that produce no (or too few) microexpressions for those techniques to be applied. *Robust to countermeasures* shows that all of the techniques apart from ST and Microexpressions have a vulnerability to spoofing. Although this has not been published for Voice Stress, because it is stress-based it has the same issues as the Polygraph. *Portability* indicates that all of the techniques except fMRI are sufficiently portable to be set up at a reasonably well serviced border crossing point (mains electricity required). *Use in home* shows that only ST and Automatic Microexpressions have the potential to be used in the traveller's home for a pre-interview. *Use in field* indicates that only ST, Polygraph, Voice Stress and Automatic Microexpressions could be used at a reasonably well serviced border crossing point. *Capital cost* indicates that only fMRI is prohibitively expensive, although throughput on other techniques (e.g. Polygraph, EEG) may also render then cost-ineffective. *Interview cost* shows that a combination of time and cost of skilled interviewers penalises all of the techniques except ST and Automatic Microexpressions. Although Voice Stress ought to be cheap, the UK government trials of Nemesysco were strikingly expensive. *Licensing issues* only affect Automatic Microexpressions. There are many existing patents for automatic methods of facial action coding (e.g. Bartlett et al, 2014) so either novelty would need to be established or a technique licensed. The SDK they used for facial recognition, PittPatt, has been acquired by Google and the long vector technique is covered by the ST patent.

Therefore the weight of evidence in Table 6 supports the use and evaluation of ST technology in developing the ADDS component of iCROSS.

3.3.9 Avatars and Supporting Technologies

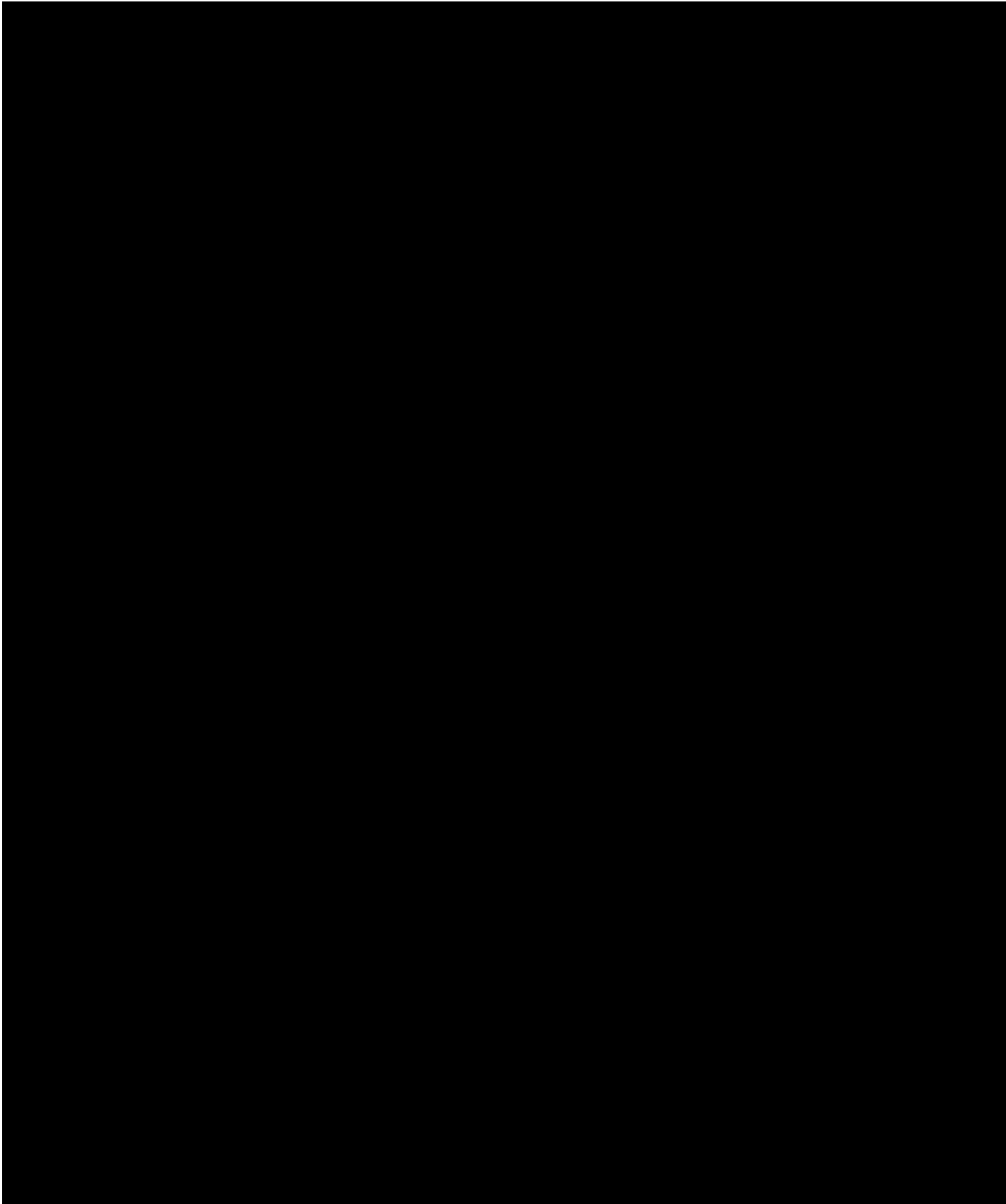
Border control officers' tasks rely on bilateral human interaction such as border control agents interviewing an individual using verbal and non-verbal communication to both provoke response and interpret the traveler's responses. ADDS is powered by Silent Talker, a system capable of semi-automating that process by quantifying the probability of deception on the part of the interviewee. However, to maximize the potential impact of ADDS, it would be beneficial to utilize this system not

only to collect data completely automatically on the potential of deceitful behaviour by a traveler at the pre-crossing stage.

To achieve this, an advanced border control agent avatar will be created. This will be instantiated per traveler and will be personalized to communicate with the traveler including utilizing subtle non-verbal communication cues to gauge response to them. A strong focus will be on identifying the impact on non-verbal communication expressed by the avatar that may also be personalized based on information available already for the traveler (ethnicity, gender, educational level etc.) to the performance of ADDS.

Furthermore, completely automating parts of the interview questions will enable shifting some of those to the pre-crossing phase thus resulting in considerable time and monetary savings at the BCP while increasing security

[REDACTED]



3.3.10 Summary of Avatars and Supporting Technology applicable in iCROSS



3.4 Biometrics

Biometrics are widely used today, from our phones to all devices that require an authenticate protocol with more reliable security means than a single PIN code. Therefore, most individuals are quite familiar with such biometric technologies and rarely notice an extra security layer when a biometric authentication is present. However, not all problems have been solved, biometrics are only in a limited number of devices and consist mostly of fingerprint readers and some photo recognition capabilities (for example, facial recognition has not been implemented in mobile phones, so far).

We are experiencing a demanding for biometrics in new business models like online payment, credit cards payments, banking solutions, live concerts, airports, marketing, etc. and, of course, **public security**. This is now a major concern for all countries and societies; moreover, in the current situation where terrorism has become a dire and global concern, biometrics emerges as innovative means which could greatly contribute to improve the situation by tackling related threats.

Another domain where biometrics appear as promising technologies is **border control/management**. This field requires, for obvious reasons, the maximum-security level with a limited operational cost and a high speed of processing. Solutions based on cards (swipe or contactless) are not the best option if a high security level with a minimum impact in time of transit is the goal. Under these circumstances, biometrics arises as the best choice given that they combine a human biometric feature with a fast answer from security systems (Jain et al., 2008) (Ratha et al., 2008).

In order to establish a classification of levels of security – in border access control – for different currently available technologies the following list could be proposed:

1. Magnetic swipe card
2. Contactless card in 125 KHz (passive reading)
3. Contactless card in 13,56 Mhz (active reading)
4. Contactless card in 13,56 Mhz and PIN code (active reading)
5. Fingerprint Readers
6. Palm Vein Readers
7. Facial, voice and iris recognition
8. Retina recognition

[1: minimum security level – 8: maximum security level]

[1-4: Non-biometric. 5-8: Biometrics]

3.4.1 Fingerprint

Fingerprint technology is the most widely known biometric technology and most commonly used in commercial applications. These technologies are based on a sensor to capture the fingerprint pattern and convert it into a simple mathematical model with 8-10 matching points. Fingerprint readers can be of different nature – optical, capacitive, ultrasound, thermal – each technology has ups and downs however capacitive is the most widespread solution.

Optical fingerprint readers require an extra space that could represent a challenge if they are to be used in portable devices like smartphones, tablets and laptops. Capacitive readers could be assembled into these devices because they are based in flat capacitors that could be adapted to any market device.

Nowadays fingerprint readers are considered to be the lowest security level in biometrics due to several factors. A fingerprint is easy to cheat; a non-expert person following a YouTube video could deceive 95% of fingerprint readers. Also, fingerprint readers require a physical interaction between users and the system, which very often is regarded as unwelcoming, even irritating by them.

Still, this technology remains widely used because is very cost-effective and easy to install (even if clearly does not provide a high-standard security level) (ieee.org 2016) (fbi.gov 206).

3.4.2 Palm Vein readers

The Palm Vein technique of biometric identification that uses the analysis of the patterns of blood vessels below the surface of the skin. The security level is higher than a fingerprint. However, readers are usually bigger and expensive than fingerprint and require large space therefore not recommended in turnstiles and access control facilities.

The BioSec palm vein scanning technique uses near infrared light to illuminate the vein pattern below the skin for an IR optic. The IR light is absorbed by the blood; so the complete vein pattern will appear black for the IR camera. Using this image, ~5 000 000 reference points is created and based on this a coordinate system is created and converted to an encrypted hash code. The image will be irrevocably deleted inside the sensor, within a black box.

The benefits of the palm vein pattern based authentication:

- to avoid authentication, the hand has to be cut off, or partially “destroyed”
- FAR 0,00008%, FRR 0,01%
- authentication time 1 second
- very difficult to cheat, as the vein pattern cannot be reproduced or copied

The use of the sensor itself is contactless. Compared to other high security solutions, the BioSec palm vein based authentication is a cost effective.

Compared to other devices, the personal vein ID cannot be stolen and the use of the palm vein scanner is contactless, therefore if a person identifies him/herself then the vein ID cannot be stolen and used elsewhere, since it leaves no trace.

The device is connected via one USB cable, therefore simple to install and the size of the sensor itself is ~30*30*30mm.

3.4.3 Voice Recognition

Voice recognition comprises several technologies like voice fingerprint, audio fingerprint and content analysis. Voice fingerprint creates a unique print of a human voice with 10 thousand parameters (thousand percent more parameters than fingerprint) and could be used to match like a regular print. Audio fingerprint uses voice biometrics to spot a single word or a sentence in a conversation. Finally, content analysis searches topics in a given conversation, instead of a single word or sentence.

A voice fingerprint is generally used to identify a person in a speech, conversation or phone call. The security level is close to facial and iris recognition and is used in many commercial applications to identify users. Standard call centres and other automated calling machines use audio fingerprint to identify numbers and single words but they do not apply voice biometrics to identify users, as this might pose important legal/ethical implications (Rabiner et al., 1993).

3.4.4 Facial Recognition

Facial recognition technologies use a standard CCTV camera to create a pattern from a human face resulting in a unique print of this person. Facial recognition requires a lot of computing power therefore, until very recently, computers could only process facial recognition in forensics. Nowadays, live facial recognition is feasible and largely used.

It is important to say that facial recognition and face detection are different technologies. Facial recognition uses eyes, nose and mouth triangle to create a single user pattern that could feed from a standard CCTV camera, while face detection is a common technology generally confused with the former (and not nearly as powerful and sophisticated) which uses face contour, typically needing frontal faces and still pictures, in order to establish a direct match with another picture.

In other words, face detection is not a biometric technology because it consists of “comparing pixels” through digital processing of images and not biometric features, therefore must be placed with regards to security on the level of active contactless card (like Mifare technologies). Windows Hello is a classic example of face detection technology (Moeslund et al., 2014).

3.4.5 Iris Recognition

Iris recognition is a high performance biometric technology which it uses the iris structure to create a unique matching pattern that will be linked with a single user. In order to capture and check this pattern a camera and lighting system (usually based on infrared) are needed. Iris technology will, in future, stand out amongst others.

Unfortunately, Iris recognition requires expensive hardware and is affected by several problems in daily, routine, use affecting performance and accuracy. Users must be placed in front of this system and specific lighting conditions are necessary (provide by the system) so many problems are related, for example, with outdoor installations.

3.4.6 Retina Recognition

Retina is another high performance biometric technology. The retina is unique and the most accurate feature in human body. A retina reader requires a high-standard camera and advanced equipment which represents an operational – and commercial – problem. In fact, no commercial solutions with real retina biometric reader are available in the market for the moment. Iris solutions

are more economical and, definitely, easy to handle therefore still retina biometrics are in the pipeline.

3.4.7 Comparative chart of biometric technologies

Table 8 provides a **comparative overview** of the previously presented technologies.

Table 8 Comparative Overview of Biometric Technologies

Biometric Technology	Security Level	Cost	Speed of detection	Accuracy
Fingerprint	Low	Cheap (\$)	Fast (<1 second)	Fair
Palm Vein Reader	High, FAR 0,00008%	Medium (\$\$)	Fast (<1 second)	Excellent
Voice Fingerprint	Medium	Expensive (\$\$\$)	Medium (3-5 seconds)	Excellent
Facial Recognition	High	Medium (\$\$)	Fast (<1 second)	Excellent
Iris Recognition	High	Expensive (\$\$\$)	Medium (3-5 seconds)	Good
Retina Recognition	Extremely High	Not commercial	Not commercial	Excellent

3.4.8 State of the Art in Facial Biometrics

After reviewing a number of biometric technologies in the previous section, we will draw our attention now to **Facial recognition**, given the prominent role it will have in iCROSS as central component of the FMT (Face Matching Tool) module. The selection was made in search of a high security level, excellent accuracy and a fast response. Facial recognition also permits non-intrusive detection and detection of moving people. Facial recognition will be our best choice for the border control application.

Facial technologies have become popular but face detection (pixel comparison) must not be confused with facial recognition (biometric mathematical model comparison). The goal will be taking advantage of cutting-edge facial recognition solution that allow:

- Identification in less than 1 second
- Non affected by a beard, hat or glasses
- Identification in a group of moving people
- Utilization of huge databases (> 1 million people)
- Accuracy in 99.99%, more specifically, the FRR and FAR for the technology to be applied in the project is the following:

Table 9 Facial Recognition Accuracy

	FAR	FRR	Comments
Still image datasets (FERET, XM2VTS)	0.007		FAR=FRR. Controlled lighting, approximately frontal

	FAR	FRR	Comments
Challenging dataset (LFW)	0.193		FAR=FRR. Poor lighting, non-frontal, occlusions. Non-detections are accounted as false recognitions

The IP camera is also a paramount element of facial recognition. Configuration of these cameras will be key for success of facial recognition solution. The general recommend will be utilizing cameras with resolution of at least 1.3 Mpixel (3 Mpixel cameras for optimal results).

The technology to be used in iCROSS project is focused on real-time detection (although with some forensic capabilities) and the most important feature is speed (processing power) propelled by Nvidia technology present in the software to be used, which is capable of handling a million user database and identifying a person in less than a second, which makes it an excellent option to tackle the typical problems at border access control.

3.5 Hidden Human Detection Technology Tools

3.5.1 *Hidden Human Detection Technologies: Hidden Human Detection in Land Borders*

The scope of this section is to briefly present the State of the Art of the technologies and potentially available commercial tools that address the issue of adequate detection of people hidden inside vehicles, trucks, trains containers or open cargo wagons when crossing land borders. This aspect constitutes an existing problem that is continuously reported at the border control checkpoint, especially in land borders; in many cases illegal travelers hide themselves in busses, cars or trains, since they do not possess the necessary travel documents. The authorities have to detect them and they do so, mainly by visual inspection, while in certain cases without full availability of the appropriate tools to support them.

However, relevant thorough and systematic checks to all vehicles are not performed routinely, especially when traffic flow across the check points increases and rising flows of people or vehicles cross the check points. Instead, they are made occasionally or indicatively, unless dictated by official warnings, relying mostly on visual inspection and often rely on the staff's (border guards, police and custom officers) experience and perception. Although various types of relevant equipment exist on the market with various levels of reliability, a single, cost effective, prompt and easy to use technology is not yet available; advanced methods of detection such as x-ray equipment (used for trucks and containers) is too expensive to be widely implemented whilst being unsafe for human beings.

On the other hand, trafficking and illegal smuggling of human beings are severe problems which have continued to expand rapidly during the last few years. Quite often, large groups of illegal immigrants or refugees are found hidden in large trucks' containers carrying goods. Also, illegal passengers hide themselves on board freight trains (especially in bulk cargo open wagons or containers), since they don't possess all the papers for a proper border check. Nowadays, this seem to be the common case for illegal passengers, immigrants or refugees; either distinct cases of one or two illegal passengers are recorded or the massive transfer of hidden people takes place. ■■■■■

Experience shows that the dominant method of detection still seems to be the visual inspection of a car or vehicle. As it will be seen later on in this Deliverable (Chapter 4.4.2 – user responses), visual inspection can be assisted by a range of measures to control vehicles (depending on whether it is a car, truck or railway wagon) and dogs / K9 units as well. The level of the measures used depends on the risk analysis in each case based on the Border Control Officer's experience. If anything is suspicious, the vehicles may be checked more systematically and thoroughly on a second level (Second Line check) with additional tools and technologies. In extreme cases it is also possible to dismantle the vehicle.

The iCROSS project intends to address the increasing necessity of detecting hidden people in various kinds of vehicles. As it will be shown, the detection of hidden humans and illicit goods for borders and customs security is a challenging issue, and could form a whole project by itself, incorporating extensive and multidisciplinary research. A single technology for the easy, fast and effective detection of humans hidden in a variety of vehicles (cars, trucks, containers, buses, trains etc.) that can be applied in all different cases and applications, is not available yet to border guard services.

The following subsections describe briefly the most significant of the technologies used so far by presenting and emphasizing on the State of the Art, both per technology and as an overall approach.

Important Notes:

It has to be noted, that the detection of illicit goods (contraband, narcotics, nuclear weapons etc) is not within the scope of iCROSS. The project examines the possibility of detecting only human beings hidden in vehicles and especially it examines the feasibility of integrating such technological solutions to the overall iCROSS platform. However, since certain technologies are able to detect both humans and illicit goods, the presentation of the relevant State of the Art will not limit itself; on the contrary all relevant aspects will be examined for both cases. Of course, special emphasis will be given to the hidden human detection technologies which are among the general project's aims.

Since the general concept of iCROSS is to enable an effective, fast but also reliable border crossing, the relevant problem of hidden human detection also needs to be addressed. However, as denoted in the Description of Work (DoW), in the framework of iCROSS, this aspect will be tackled as a secondary target confronting the relevant necessity. In other words, the HHD tool will be an additional tool to be connected as an option to the main iCROSS platform solution; the ability to be implemented in the first level of alert will be explored, triggering a more in-depth inspection and search, paving the way for similar inclusions of the relevant various technologies in the future.

3.5.2 X-ray Systems

Current commercial solutions mainly involve x-ray detectors which can be used for any kind of vehicle, container or closed compartment. They are mainly used for illicit goods detection and in this

context x-rays can also reveal humans hidden inside vehicles. However, due to their unsafe effects for human beings, x-rays are not suitable for a more systematic usage on this specific purpose. X-rays are used largely in airport checkpoints for luggage checks. The relevant applications involve seaports, border crossings and critical facilities to combat smuggling, counter trade fraud and find hidden contraband, including explosives, weapons, narcotics etc. However, in land borders and seaport applications the whole vehicle or container should be subject to x-ray scanning.

Large commercial vendors offer integrated solutions of x-/ gamma-rays detectors for cars, trucks and cargo containers accompanied with a robust data and image analysis software. The relevant systems use high performance cargo and vehicle screening systems based on high energy X-ray scanning and radiation detection to provide material discrimination. They can reveal contraband through more than a foot of steel, identifying even heavily shielded nuclear material, from high throughput rail scanners, portals, road-ready mobiles and high energy gantries to drive-through car and scanners of entire vehicles, including occupants. In the following the most significant X-ray systems provided by the relevant vendors are presented in brief.

3.5.2.1 Vendor “Leidos”: VACIS® IP6500 FullScan Integrated Cargo Inspection System:

The VACIS IP6500 FullScan system is a powerful, practical solution for scanning cargo containers, trucks and other vehicles in high-volume operations (Leidos.com, 2016). Its x-ray imaging and radiation scanning help security personnel intercept weapons, nuclear material and other contraband hidden in containers. It can scan entire vehicles, bumper to bumper and roof to tires, including occupants. In addition, with its high throughput and small footprint, the system is ideal for seaports and other high-volume cargo facilities. The VACIS IP6500 FullScan system provides a combination of scanning features, such as:

- High-energy x-ray imaging that can reveal contraband through more than a foot of steel. It utilizes a low radiation dose, and the system can be used in very limited space.
- Material discrimination distinguishes light, organic material from dense, inorganic material.
- Radiation detection can detect, locate and identify even heavily shielded special nuclear material (SNM) with a false alarm rate of less than 1 in 10,000 — meeting or exceeding the challenging ANSI N42.38-2006 standard.
- Optical character recognition identifies each container as it is scanned.
- The system quickly integrates the scanning images and data for each container in the system database. Security personnel at viewer workstations in nearby or remote locations can view integrated images and data for any container at any time.

The VACIS IP6500 FullScan system is designed for practical operation at busy facilities. Built for high throughput, the system can scan large numbers of containers in the normal flow of traffic at gates or other checkpoints, without requiring drivers or passengers to exit the vehicle. With its small footprint and low radiation dose, the system can be used in very limited space. And by identifying radioactive isotopes, the system can greatly reduce the need for secondary inspection. The system's component technologies are now operating at ports, border crossings and other facilities around the world. The system is backed by Leidos worldwide service organization, providing high-quality installation, training, maintenance and technical support. Indicative Photos are provided in Figure 44.

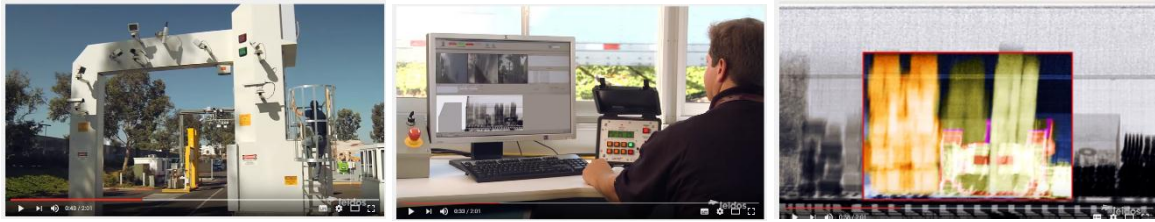


Figure 44 Leidos VACIS® IP6500 Cargo Inspection System (Official Video)

3.5.2.2 Vendor: “Rapiscan systems”: RAPISCAN EAGLE® series of products

Rapiscan Systems Cargo and Vehicle Inspection products have been deployed in a variety of government and private sector applications, winning out on the basis of their exceptional threat detection capabilities (Rapiscansystems.com, 2016). Customers can choose products from the EAGLE Series with specific features and scanners that operate in different modes to adapt to changing operational requirements; with Mobile (EAGLE M Series), Portal (EAGLE P Series), Trailer Mounted (EAGLE T Series), Rail (EAGLE R Series), Air Cargo (EAGLE A Series) and Gantry Scanners (EAGLE G Series). Indicative photos are shown in Figure 45. The products are accompanied by a powerful software suite (RAPISCAN AUTO-Z™ Detection Software) which analyzes the x-ray image data and identifies the location of High-Z material within the container, even for highly-cluttered and dense cargo not fully penetrated by the beam (i.e., partially saturated).

Among other benefits, such as speed, reliability, cost-effectiveness, and ease-of-use, Rapiscan cargo and vehicle inspection systems are also backed by the company’s global support network. All Rapiscan cargo and vehicle inspection products claim to present excellence in imaging performance, design, ease-of-use, quality, high reliability and high operator satisfaction. Rapiscan’s cargo and vehicle inspection systems are proven in challenging applications at seaports, border crossings and critical facilities around the world assisting inspectors to combat smuggling and find hidden contraband, including explosives, weapons, narcotics and weapons of mass destruction. Customers can choose products with specific features and scanners that operate in different modes to adapt to changing operational requirements.



Figure 45 Rapiscan Series of Products

3.5.2.3 Vendor: “Smiths Detection”: Cargo and Vehicle Inspection series of products

Smiths Detection product series perform Cargo and Vehicle Inspection at any location with a variety of X-ray scanners such as (Smithsdetection.com, 2016):

- Ultra-light and Compact Mobile X-ray - HCVM e35 and Towable - HCVM e35 T scanner,
- Mobile X-ray system - HCVM L scanner and Towable X-ray system - HCVM T trailer for cargo inspection including a comfortable operator’s cabin for up to 4-8 personnel respectively,

- Stationary X-ray system – HCVS Cargo inspection in a dedicated vehicle scanning facility for heavy traffic locations such as container ports and terminals,
- Drive-through portal – HCVP for screening high volumes of vehicles with a stand-alone X-ray portal where vehicles are driven through at low speed (the driver's cabin is not scanned),
- Automatic and driverless screening with HCVG where the scanner moves along the vehicle during the cargo inspection process delivering X-ray images of the entire vehicle including wheels and fuel tank,
- Scan light vehicles with HCVL suitable for inspecting occupied cars and light vehicles applying high-energy X-ray system that can accommodate high volumes traffic and can be available in drive-through or automatic conveyor models.

Indicative photos are shown in Figure 46.



Figure 46 Smiths Detection Series of Products

All product series are accompanied with various software platforms (iCMore, HCV-DMS, Z-VISUAL, DAISY) to detect and pinpoint suspicious cargo; with centralized networking & secure data to speed up the whole analysis process, and automatically detect radioactive material, with coloured material discrimination, allowing customization with favorite image settings, for fast verification of cargo.

EU related Research

European Research projects also tackled the use of X-rays images in security applications especially under the FP7 SEC-2012.3.4-1 - Research on "automated" comparison of x-ray images for cargo scanning with reference material to identify irregularities and FP7 SEC-2007-3.2-03 - Integrated checkpoints security. In this framework, the following indicative FP7 projects are mentioned:

- ACXIS (*"Automated Comparison of X-ray Images for cargo Scanning"*, FP7 Security, 2013-2017) for automated identification of illegal and legitimate cargo with X-ray images (ACXIS project, 2013).
- EFFISEC (*"Efficient Integrated Security Checkpoints"* FP7 Security, 2009-2014) which provided a more integrated approach on check points security (EFFISEC project, 2009).

3.5.2.4 Discussion on X-ray technology

X-ray systems are the most reliable commercial solution for detecting any kind of hidden contraband; the relevant systems focus mostly on detection of weapons, nuclear material, explosives and other contraband hidden in vehicles or containers since this technology penetrates easily through metal walls. However, such technology solutions require large budgets for installation and maintenance and thus are too expensive to be suited for every kind of border control cases. On the other hand, it is difficult to deploy this technology in all border control scenarios since such systems require large and demanding installation facilities. Thus, although these systems are best suited for airports and even seaports with large facilities for containers, they are less applicable at land

borders, especially for countries with extended border lines - limiting their deployment to large border control facilities.

X-ray, gamma and neutron imaging systems that can be used to inspect vehicles/containers have been widely studied in terms of scientific research [(Duan et al., 2009), (Liu et al., 2008), (Zentai, 2008) and (Zhu et al., 2010)]. However, they generate radiation which in large doses is unsafe for human beings and these could also be problematic in the presence of biological material or sensitive integrated circuits (Rogers et al., 2016). Furthermore, apart from being expensive, these systems are rather slow and range-limited. In land border and seaport applications the whole vehicle or container should be subject to scanning, scanning time cannot be too fast and also the time needed for image processing and material discrimination should be taken into account. Although these scanning times can be affordable in low-traffic cases, they can cumulatively result in quite large border crossing times and long vehicle queues.

3.5.3 K9 Units and artificial sniffers - gas detectors

Apart from X-rays, portable or desktop commercial products can also be found in the market for illicit goods detection (mostly explosives). These are mainly based on chemical liquid agents and trace detectors, such as the Rapiscan's DETECTRA HX product (Rapiscansystems.com, 2016) along with the IONSCAN 500DT and IONSCAN 600 desktop systems offered by SmithsDetection Inc. (Smithsdetection.com, 2016). However, these systems are mainly meant for detecting and identifying explosives and narcotics while maintaining high sensitivity; the same cannot be said for hidden humans' detection. At present, profiling and detection dogs have proven to be the most effective methods to detect humans hidden inside vehicles.

A police dog, known as a "K-9" or "K9 unit" (a homophone of "canine") in some English-speaking countries, is a dog that is specifically trained to assist police and other law-enforcement personnel in their work (Figure 47). Their duties include searching for drugs and explosives, searching for lost people, looking for crime scene evidence, and protecting their handlers. Police dogs must remember several hand and verbal commands (New York State Department, 2014). The most commonly used breed is the German Shepherd. The police dogs show a wide specialization: Sentry dog and attack dog, Search and rescue dog, Detection dog or explosive-sniffing dog, Arson dogs, Cadaver dogs. Detection dog or explosive-sniffing dogs are used to detect illicit substances such as drugs or explosives which may be carried by a person in their effects. In many countries, Beagles are used in airports to sniff the baggage for items that are not permitted; however, they require close proximity of dogs to vehicles/containers and the detection may take significant time.



Figure 47 Police Dog in Wisconsin (Source: wikipedia) and GASDATA CO2 sensor (source <http://www.gasdata.co.uk/>)

On the other hand, products based on CO₂ sensors are offered commercially by vendors such as GASDATA Ltd (UK) in order to tackle the detection of stowaways in a variety of civil, law enforcement and military situations (Gasdata.co.uk, 2016). As human beings exhale carbon dioxide it is possible to analyse gas samples taken from enclosed spaces to indicate if people are hidden or trapped. Gas Data's CO₂ detectors has been used by security organisations around the world in a variety of applications including: stowaway detection at ports, searches for fugitives and location of earthquake victims. The Gas Data GFM226 Hidden Person Stowaway Detector is a portable carbon dioxide detector developed especially for the detection of people hiding or trapped in confined spaces such as trailers, rooms or vehicles (Figure 47). Working primarily by detecting the elevated levels of carbon dioxide and reduced levels of oxygen in human breath, the GFM226 is used in a variety of different security, transport and search and rescue applications (Gasdata.co.uk, 2016).

Artificial systems resembling or complementing dogs, in turn, have been thoroughly studied, for example in the framework of EU research projects, targeting equally effective technological solutions. FP7 Security Calls addressed the needs for "Innovative, cost-efficient and reliable technology to detect humans hidden in vehicles / closed compartments" (SEC-2012.3.4-4), along with "Artificial sniffers" (SEC-2011.3.4-2). Among the solutions suggested, the following projects can be highlighted, focusing on detecting odours of hidden people in containers, illegal substances, drugs, explosives etc.:

- SNOOPY ("*Sniffer for concealed people discovery*", FP7 Security, 2014-2016) incorporating a handheld artificial sniffer system for hidden persons and illicit goods, based on air sampling sensor arrays of gas, vapour and human perspirations like carbonic acids, aldehydes, thiolic and nitrogen compounds and the CO₂ as the human breathing product (SNOOPY project, 2014)
- HANDHOLD ("*HANDHeld Olfactory Detector*", FP7 Security, 2012-2016) for developing artificial olfactory sniffers complementing dogs (HANDHOLD project, 2012)
- SNIFFER ("*A bio-mimicry enabled artificial sniffer*", FP7 Security, 2012-2015) with bio-mimicry biosensors (SNIFFER project, 2012)
- SNIFFLES ("*Artificial sniffer using linear ion trap technology*", FP7 Security, 2012-2015) with linear ion trap mass spectrometry gas sensors (SNIFFLES project, 2012)

As denoted earlier, canine inspections are effective, but they require close proximity of dogs to vehicles/containers and the detection may take significant time. CO₂ sensors on the other hand, detect the carbon dioxide emission, and then the breathing cycle of a human subject. However, the response time of a CO₂ sensor is very slow. Additionally, the sensor has to be very close to the subject in order to obtain reliable data for adequate processing since the relevant sensor is very directional [(Klock, 2006) and (Rao, 2012)]. However, the artificial sniffers and especially the CO₂ sensors can be combined with other sensors detecting i.e. human vital signs such as heartbeat monitoring sensors.

On the other hand, usually in land borders, security personnel establish contact with the passengers and vehicles in limited space (i.e. entering the bus or train) and in many cases without requiring drivers or passengers to exit for passport control; thus the relevant checks take place through the inspection and rely mainly on the guards' experience and perception. Moreover, in cases with high throughput and rising cross-border flows, time is limited for in-depth controls, therefore vehicles and containers are not systematically checked for hidden persons; thus, dogs and artificial sniffers although most reliable, may not be the most suitable solution in rising flows, increasing the need for other types or combination of sensors and/or portable devices.

3.5.4 Non-ionizing Electromagnetic (EM) radiation – radars and microwave sensors

Non-ionizing electromagnetic (EM) radiation has also been thoroughly examined in terms of relevant applications. A mapping of the relevant recent and past research suggestions on non-ionizing EM radiation for humans' detection, starting from previous decades, can be summarised as follows:

- **CW Doppler radar**, which can be used:
 - as Life Detectors of breath, slight movements and / or vital sign detection.
 - as see-through-wall radar, entrance security monitoring, border patrol and other relevant security requirements.
 - At various frequencies from X-band (10 GHz) and higher to lower bands such as the lower microwaves bands (2.5GHz and 1150 MHz) or even UHF (450 MHz) depending on the penetration requirements and the materials in between.
- **Multi-frequency microwave radars**, which detect human movements and gestures through micro-Doppler signals, at short or long ranges.
- Recent use of **UWB pulses radars** which show high penetration capability.
- **Millimetre (mm-) wave passive and active imaging / radars**; capable of remote detection of metallic and non-metallic objects and contraband concealed beneath clothing, enabling “through-the-wall imaging systems (TWIS)” and remote observation of humans for military and law enforcement personnel. **Passive mm-wave radars** are better for outdoor detection and for body concealed weapons
- **THz technology**; an emerging candidate for concealed non-metallic weaponry.

We will now briefly examine the most important of the above technologies:

3.5.4.1 Microwave Doppler radars and Life Detectors

Doppler radar produces velocity data of “targeted objects” at a distance, by illuminating them with a microwave electromagnetic (EM) signal (forward) and exploiting the frequency shift of the returned (EM echo) scattered signal due to the target’s motion. The Doppler radar is able to detect and track moving targets. The target velocity is a function of the frequency shift between the two signals (according to the well-known Doppler Effect).

Doppler radars at microwave frequencies can have low power consumption, be light-weight, inexpensive and mounted in small objects or vehicles. In contrast to optical or infrared (IR) systems, Doppler radar can work in harsher conditions such as at dusk, in rain and snow. In contrast to ultrasound systems, it can detect small sized obstacles such as wires more accurately, providing a sensing range up to several Km. Signal processing algorithms are applied to measure range/velocity and distinguish targets from clutter; nevertheless, detection ability depends heavily on the target’s size and shape (Radar Cross Section (RCS)) which may result in challenging aspects.

Radar systems operating at a wavelength of a few mm can provide good enough visibility in harsh conditions. CW Doppler radars use a single wavelength as a Continuous Wave (CW) forward signal; in other words, a single frequency (one tone) is used. Microwave signals within a 3 GHz - 30 GHz frequency range seem to be optimal while X and K-band (12-27 GHz) systems provide good sensitivity for obstacles with small RCS. Low RCS makes the detection within cluttered environments very demanding. Different targets are expected to present a wide range of different RCS profiles and RCS values of complex targets can fluctuate an order or two of magnitude depending on the orientation. The detection of low RCS moving targets can be accomplished,

although with difficulty, by measuring their motion and other subtle aspects of each echo and applying robust signal processing and machine intelligence. To this end, Doppler based techniques constitute different approaches depending on the particular case examined.

In the past, several researchers have suggested the use of CW Doppler radar as a “Life Detector module” to detect trapped living persons within collapsed buildings based on their breath or slight movements [(Misra et al., 1986), (Lin, 1992) and (Aggelopoulos et al., 1996)]. Over time, life-detection radar for vital parameter detection evolved into a highly useful and important application and recently, an increased attention to radar based life detection systems can be observed. Quite recently, NASA/JPL’s “FINDER Search and Rescue Technology” based on EM radar detecting victims’ tiny motions (breathing and heartbeats) helped save lives of trapped people under destroyed building in Nepal earthquake on April 2015, (NASA JPL, 2015).

Apart from searching for trapped people in collapsed buildings, the CW Doppler radar can also be used for contactless monitoring of patients’ vital signs and has also attracted the interest of organizations requiring high security. To this respect, the relevant and current research includes emerging applications such as see-through-wall radar and airport security monitoring, and border patrol along with entrance security to search for criminals hiding behind various covers or vehicles.

Penetration depth and spatial resolution are the main tradeoffs of Doppler radar’s performance as the most difficult material to penetrate from the electromagnetism point of view is reinforced concrete. Electromagnetic waves cannot penetrate fully closed metallic objects or walls, thus, strong metallic components inside normal and ordinary materials may complicate the relevant penetration and subsequent processing. The most important parameter that affects penetration depth and spatial resolution in respect to the set target to be detected is operation frequency.

In this review, the selection of operation frequencies is a critical issue depending on the specific application and needs to be thoroughly investigated. It is known that, as frequency goes higher (i.e. X-band) excellent spatial accuracy of detecting very slight movements (i.e. breath) of persons is achieved although penetration depth is limited especially concerning materials involving metallic elements. On the other hand, lower frequencies (VHF bands) provide much higher penetration depth but only large-scale movements of human body could be detected (i.e. an intensive movement of hand). Finally, in order to achieve proper reception, the breath frequency needs to be acquired in front of a human; thus in practical situations various angles in terms of the vehicle – radar axes need to be looked at while the sensitive range could be expanded by using more or bistatic systems.

More recent advances have been suggested using Ultra-Wide Band (UWB) radars with pulse transmission (Chao, 2012). The reason is that such applications provide high material-penetration capability, good immunity against multipath interference and large bandwidth which allows a better separation between target and clutter but only large-scale movements of human body could be detected (i.e. an intensive movement of hand). Finally, in order to achieve proper reception, the breath frequency needs to be acquired in front of a human; thus in practical situations various angles in terms of the vehicle – radar axes need to be looked at while the sensitive range could be expanded by using more or bistatic systems.

3.5.4.2 Multi-frequency microwave radars

Multi-frequency microwave radar systems have been studied, (Narayanan et al., 2014) for detecting humans and classifying their activities at short and long ranges using the characteristic micro-Doppler signals to distinguish between different human movements and gestures. Doppler measurements are used to detect and range humans and distinguish between different human movements at different ranges. Although this multi-frequency microwave radar system is capable of

through-wall applications at short distances, it is clear that it cannot see through metal walls since the EM radiation cannot penetrate metallic objects.

The system incorporates two main sub-systems: The short-range radar sub-system, which operates in the S-Band frequency range (2-4 GHz), is meant for through-wall applications at distances of up to 3 m. It utilizes two separate waveforms (a wide-band noise waveform or a continuous single tone) which are selected via switching. The long-range radar sub-system operates in the W-Band millimeter-wave frequency range (75-110GHz) and performs at distances of up to about 100 m in free space and up to about 30 m through light foliage. It employs a composite multimodal signal consisting of the two waveforms, again a wide-band noise waveform and an embedded single tone, which in turn are summed and transmitted simultaneously. Matched filtering of the received and transmitted noise signals is performed to detect targets with high-range resolution, whereas the received single tone signal is used for the Doppler analysis.

3.5.4.3 Millimeter (mm-) wave passive and active imaging - Passive microwave / mm-wave radars

Millimeter wave passive imaging technology, on the other hand, offers the opportunity for rapid and remote detection of metallic and non-metallic weapons, plastic explosives, drugs, and other contraband concealed under multiple layers of clothing without the necessity of a direct physical search (Huguenin, 1997). The ability of millimeter waves to penetrate many common building materials permits the remote observation of people and other objects within a room enabling “through-the-wall imaging system” (TWIS) applications for military and law enforcement personnel, (however not through metal walls).

This purely passive imaging technique relies solely on the existing natural emissions from the scene objects, does not expose the person to any man-made radiation, and is therefore completely harmless to the person being observed and to all others in the area. Screening can be done remotely and with as much discretion as the situation requires. The passive imaging approach to the detection of concealed weapons and contraband hidden under people's clothing works well at millimeter wavelengths because of a fortunate convergence of a number of key factors: (1) adequate resolution in a reasonable sensor size; (2) high transparency of virtually all clothing; and (3) the extraordinarily high emissivity of human flesh compared to the vast majority of other materials. Longer (microwave) wavelengths are impractical because of sensor size and resolution issues, and shorter (infrared) wavelengths are impractical because of the poor transparency of most clothing.

The ability of millimeter wave emissions to penetrate many common building materials permits the remote observation, using active millimeter wave sensors, of people and other objects within a room from outside of that room. The resulting through-the-wall 'live' video images of people and furnishings will indicate their location, posture, and activity within a room which should be valuable knowledge to military and law enforcement personnel (i.e. Special Operations) prior to their entering that room. Millimeter wave radar imaging systems based on passive MillivisionR camera technology have been developed by Millimetrix (and other members of the MIRTAC TRP consortium) for Through-the-Wall Imaging System (TWIS) applications as included in (Huguenin, 1997).

Passive microwave radars are much better for outdoor use (not through walls). Passive millimeter wave (PMMW) imaging has also been explored for indoor usage and detection of concealed weapons in human body. The passive millimeter wave (PMMW) imaging is often successful for outdoors as radiation of natural sky (“cold source”) provides the required contrast for imaging. When this

method is used indoors, to detect i.e. weapons hidden under clothing has failed since the contrast between the target and the subject is not being obvious due to the lack of sky radiation.

An active illumination provides the desired contrast for the image recognition, however, it causes the image to “blind” and “flicker” resulting in poor quality of imaging and target identification. Despite that, a PMMW imaging security system for indoor usage has been reported (Shi and Yang, 2014). This system includes a front-end array consisting of a 94 GHz imaging radiometer, eight Ka-band sources with discrete frequency and discrete radiation direction to radiating harmonic illumination and a large-diameter parabolic antenna for convergence of target radiation. The system provides affordable energy “like noise” radiation, avoiding an image’s glint under coherent radiation while the results obtained from experiments on indoor detection of concealed weapon on the human body validated the theory of proposed imaging systems, its feasibility and practical utility.

3.5.4.4 Terahertz (THz) Technology

Terahertz (THz) technology is also an emerging candidate for security screening to image threat items such as explosives and nonmetallic weaponry when concealed beneath clothing (Tribe et al., 2004). FP7 Security Calls addressed the relevant needs in a more general technological point of view through “Further research and pilot implementation of Terahertz detection techniques (T-Ray)” – topic SEC-2012.3.4-5. In this framework, the following research projects are highlighted:

- CONSORTIS: “*Concealed Objects Stand-Off Real-Time Imaging for Security*”, FP7 Security, 2014-2017, (CONSORTIS project, 2014)
- TERASCREEN: “*Multi-frequency multi-mode Terahertz screening for border checks*”, FP7 Security, 2013-2017, (TERASCREEN project, 2013)

From the above research projects, it has been shown that the relevant THz technologies are not directly used for detecting humans hidden inside vehicles / containers, since they focus on items such as weaponry when these are concealed beneath clothing. However, by using Terahertz technology to detect concealed objects carried by hidden people and body-borne threats they can result in hidden human detection in an indirect manner.

3.5.5 Geophones and their applications as heartbeat detectors

Geophones and hand-held detection devices of similar type are also used, assuming that the item of interest inside a vehicle/container has good mechanical coupling with the vehicle. Geophones are highly sensitive motion transducers that are used by seismologists and geophysicists for decades (Brincker et al., 2005). A geophone is a device that converts ground movement (velocity) into voltage, which may be recorded at a recording station. The deviation of this measured voltage from the base line is called the seismic response and is analyzed from the structure of the earth (Wikipedia, 2016). This translation of the ground movement into voltage can be easily read by a microcontroller.



Figure 48 ION Sensor SM-24 Rotating Coil Geophone

Geophones have historically been passive analog devices and typically comprise a spring-mounted magnetic mass moving within a wire coil to generate an electrical signal (Reynolds, 2011). Today's geophones are sophisticated measuring devices and are based on a coil suspended by springs in a magnetic field, within a steel case, as in Figure 48. When vibration of any sort moves the case, the coil remains stationary due to its inertia. This movement of the case in relation to the stationary coil generates an electrical voltage proportional to the velocity of the coil with respect to the case, with displacements as low as nano-meters (ION Sensor, 2016). Recent designs have been based on microelectromechanical systems (MEMS) technology which generates an electrical response to ground motion through an active feedback circuit to maintain the position of a small piece of silicon (Wikipedia, 2016). The response of a coil/magnet geophone is proportional to ground velocity, while MEMS devices usually respond proportional to acceleration. MEMS have a much higher noise level (50 dB velocity higher) than geophones and therefore can only be used in strong motion or active seismic applications. The majority of geophones are used in reflection seismology to record the energy waves reflected by the subsurface geology. In this case, the primary interest is in the vertical motion of the Earth's surface and many competitors are present in the market. Geosource Inc. (MD-79-8Hz model), ION's Sensor Inc. (SM-24 model) and other vendors have been providing geophysicists worldwide with quality precision geophones designed to offer the highest performance in 2-D & 3-D seismic exploration with bandwidth from 10 Hz up to 240 Hz, meeting the seismic industry's demands for tight specification tolerances.

However, despite all the above, the same technology, used for detecting the occurrence of earthquakes, can be applied in a similar concept for human presence detection and thus it can tackle the aspects of illegal immigrants and human trafficking. To this end, Geovox Security Inc. / ONEX Technologies Inc. (Geovox Onex, 2015) developed a system known as the Advanced Vehicle Interrogation and Notification (AVIAN) Heartbeat Detector.

The AVIAN exploits the fact that human heartbeats vibrate at a specific frequency and is non-Intrusive. To this end AVIAN uses four geophone sensors and a small computer to analyze the vibrations of a vehicle, before using an algorithm to interpret the data and decide whether a human is present on board. It does this by locating the shockwave generated by a human heart, which is transmitted through any surface that the body is in contact with. The sensors are lightweight and can be applied to any hard part of a vehicle's chassis, so that the vehicle does not need to be opened up in order to be inspected, as shown in Figure 49. It is important to position the sensors on a flat metal surface on the vehicle's frame; for a large 4-axle vehicle with a full load all four sensors are used.



Figure 49 AVIAN Heartbeat Detector by ONEX SA - Source: Geovox.com and ONEX SA

From the above analysis, it is seen that Geophones constitute a very good basis to start with especially when considering a combination of sensors to form an integrated portable device. The conventional geophone's ratio of cost to performance, including noise, linearity and dynamic range is unmatched by advanced modern accelerometers. Furthermore, geophones require intimate

contact with the vehicle/container which in the majority of cases can be feasible [(Klock, 2006) and (Gamble, 2002, US Patent)]. However, the problem of this sensor is that it measures velocity, and that the linear frequency range is limited to frequencies above the natural frequency, typically at 4-12 Hz. To tackle this, it has been shown that the sensor signal can be digitally linearized, 2 decades (100 times) below the natural frequency obtaining a sensor that allows the user to measure displacement, velocity or acceleration with high sensitivity and large dynamic range (Brincker et al., 2005).

3.5.6 Metallic Containers Case: Acoustic (Sound) Sensors

Electromagnetic waves cannot penetrate metallic structures and this is a real challenge especially in the cargo containers scenario where detection of people hidden in containers is targeted.

The metallic chassis of fully closed compartments such as containers reduce largely the penetration depth. In many cases, they are not fully electromagnetically shielded and thus leakage through their walls or doors may, in certain cases, enable detection with a high sensitivity receiver despite the high increase in losses. Again, operation frequency is a key parameter as denoted in the previous section. However, this is not always the case and thus other technologies need to be applied in such situations. The metallic cargo-container shell is constructed from a derivative of carbon steel, which precludes the use of electric and magnetic techniques due to the high electrical conductivity, magnetic susceptibility, and variable thickness [(Narayanan et al., 2014), (Shi and Yang, 2014), (Changzhi et al., 2009) and (Klock, 2006)].

The high density of fissile materials in contrast to common commercial goods has also suggested that precise measurement of the gravity field that is produced by the cargo contents may provide an alternative inspection technique to identify high-density regions only [Kirkendall, 2007]. Nevertheless, this technique may result in expensive installations even when compared to the expensive X-rays facilities.

Tackling the above issues and limitations, the best possible technology allowing for cost-effective portable devices to detect humans hidden inside metallic containers seem to be the acoustic sensors (sound or ultrasound). Sound penetrates metal surfaces or metallic walls unlike the EM radiation that is unable to do so. Thus, the interior of a metallic container can be inspected using an acoustic source of sufficiently low frequency so as to effect penetration and sonification of the subject vehicle/container (Konopka, 2012, US Patent). The methods that can be implemented are case dependent and include both passives and active ones; the passive methods mainly use dynamic microphones while the active ones refer to the use of a transducer (acting as emitter) and exploiting the Doppler effect of the returned echo in the relevant acoustic spectrum.

Acoustic sensors have many advantages that include non-line-of-sight, omni-directionality, passiveness, low-cost, and low-power, weight and size, playing a potential key role in situational awareness as well. They can provide detection, direction finding, classification, tracking, and accurate cueing of other high-resolution sensors. However, acoustic sensing is highly dependent on the environmental conditions where sources of acoustic attenuation include e.g., temperature, wind speed and wind direction. By mounting acoustic sensors (or arrays) on i.e. the vehicle under inspection, propagation losses due to the environment are mitigated. Furthermore, acoustic sensors, do not depend on the size of the target, but rather on its acoustic signature. Due to the fact that sound penetrates metal walls and acoustic sensors are sensitive to small and slow motions, in principal they can detect stationary persons by breathing motion alone. Other attractive features (however case-dependent as well) include: high-resolution locating and tracking; portability; easy preparation and deployment; near-real-time data processing and display. These features can

provide a stand-alone through-the-wall surveillance capability and/or an excellent complement to a radar sensor.

It should be mentioned that, as will be presented later, there have already been accelerated research efforts on the exploitation of acoustic waves in surveillance and target recognition resulting in a surge in relevant digital signal processing technology. Higher harmonics in the acoustic spectrogram of a target, are shown to be useful for estimating the target's features such as location and speed due to the Doppler Effect in the relevant acoustic spectrum. Benefits of employing higher harmonics in the computations are brought out and models for the time variation of the Doppler frequency have already been proposed for a variety of purposes (Sadasivan et al., 2001). The acoustic signal propagation characteristics of a target are of particular focus due to the fact that real-time computations on such signals could be conveniently carried out with modern digital signal processing hardware and advanced algorithms. Whereas, an array of microphone sensors could be deployed for more advanced quantitative analysis, the signal from a single microphone is adequate for preliminary estimation requirements.

Furthermore, in order to enhance performance through metallic containers, quite recent advances (Felber, 2015) presented the feasibility of acoustic sensor technology for the detection of people hidden inside metallic containers within a low cost implementation. High power acoustic pulses are used at one or more discrete frequencies while implementing the same Doppler Effect principle for tracking people behind metal walls. In the framework of this work, a high-power acoustic sensor, capable of detecting and tracking persons through steel walls of cargo containers, trailer truck bodies, and train cars, has been developed and demonstrated. The sensor is based on a new concept for narrowband mechanical-impact acoustic transmitters and matched resonant receivers. The lightweight, compact, and low-cost transmitters produce high-power acoustic pulses at one or more discrete frequencies with little input power. The energy for each pulse is accumulated over long times at low powers, like a mousetrap, and therefore can be operated with ordinary batteries and no power conditioning. An impact-transmitter and matched-receiver system detects human motion through thick walls with only rudimentary signal processing. This acoustic through-the-wall sensor is capable of remotely and non-intrusively scanning steel cargo containers for stowaways at a rate of two containers per minute.

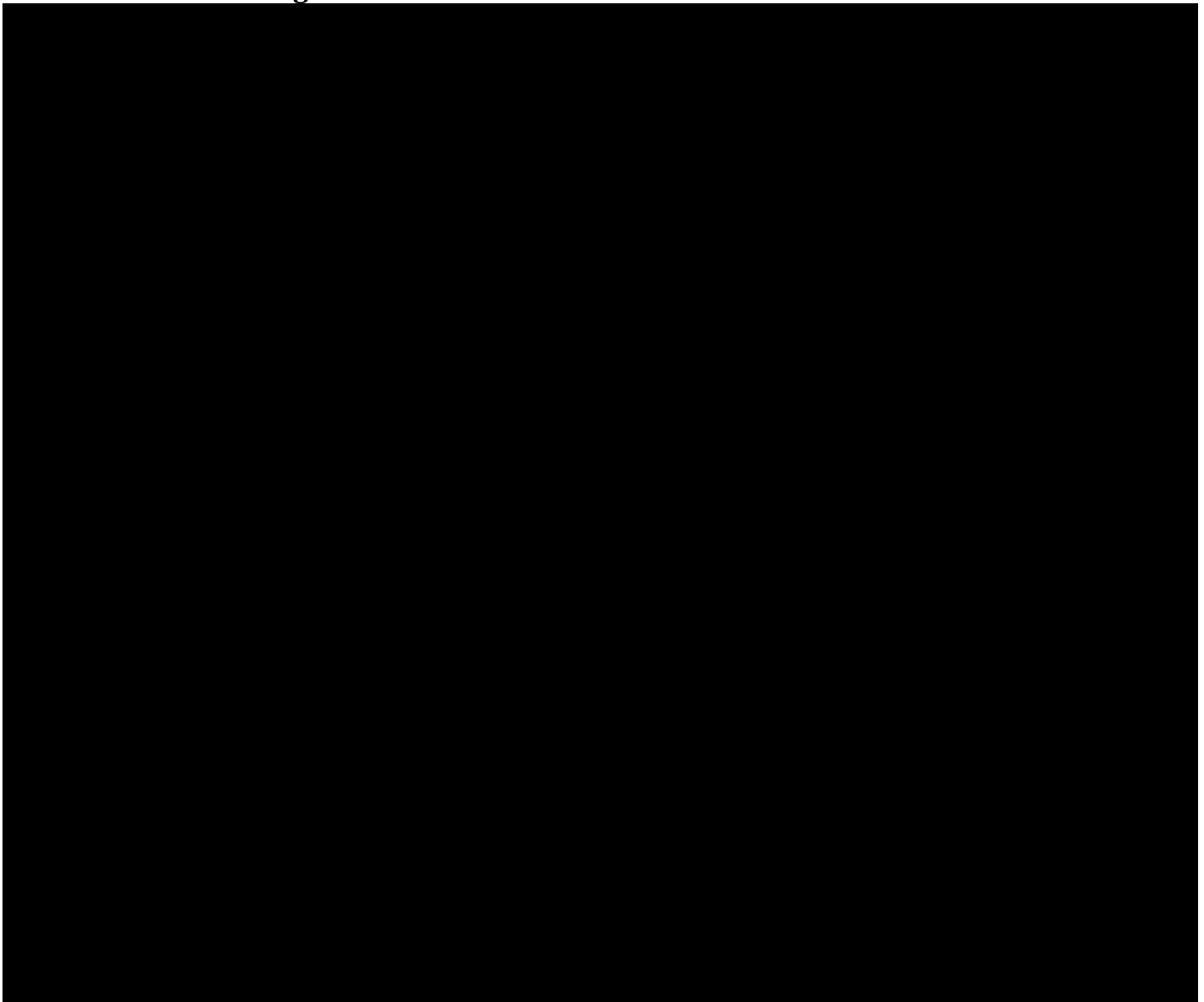
3.5.7 Combination of Sensors

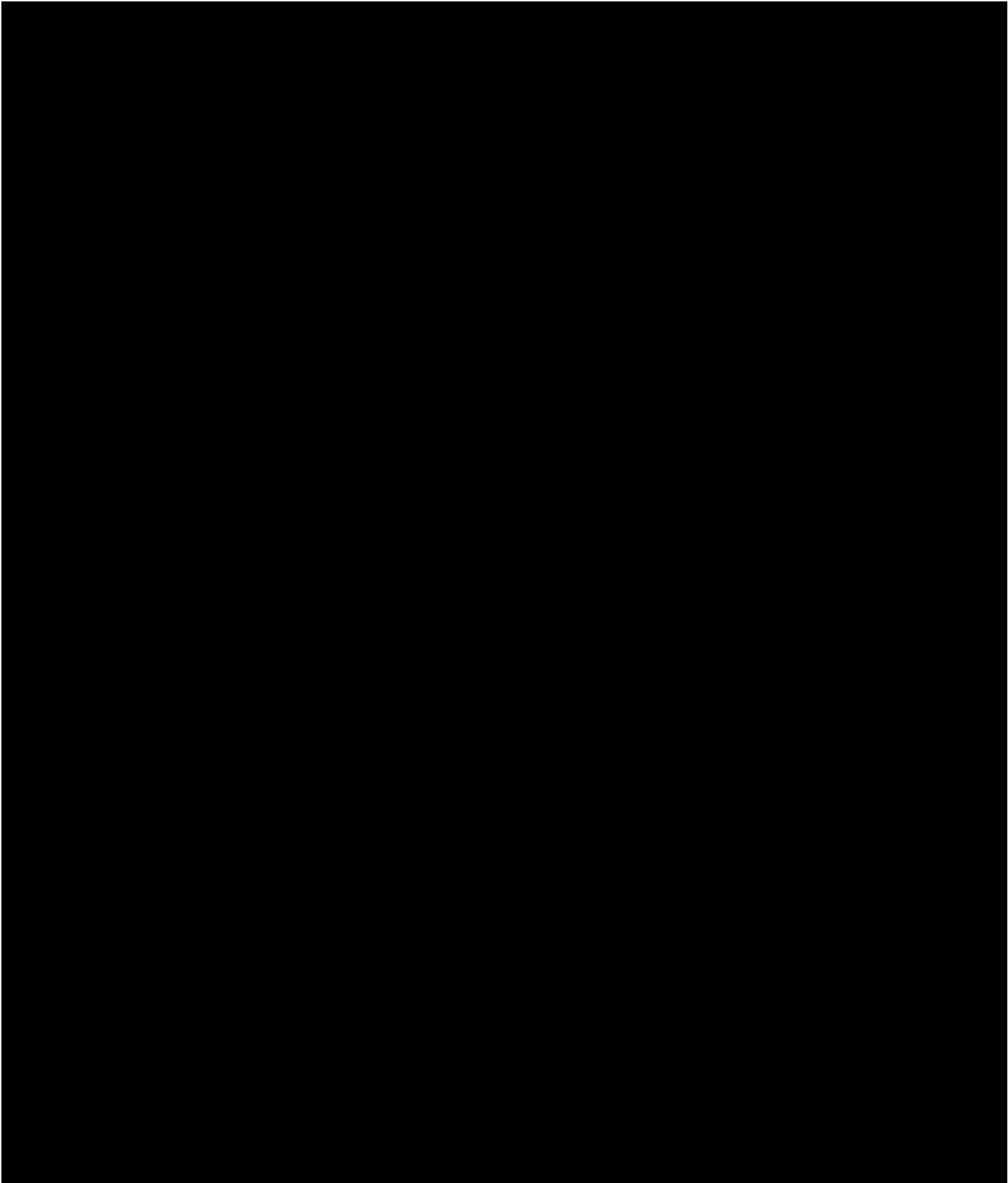
Because of the limitations discussed so far, even though a number of systems have been proposed, human presence detection in vehicles/containers still remains an active problem for which there are no completely suitable solutions. In order to fill this void, combination of other techniques is suggested; e.g. the implementation of "smart" containers, employing a variety of sensors to detect and communicate what happens to the container during its travels (Whiffen, 2005) and if the container has been opened without authorization during the travel. The actual combination of various kinds of the sensors discussed so far, has been proposed as well. In any case, newest technology trends in a broader range of applications show that detecting moving targets with low RCS is quite feasible through the implementation of mixed techniques, involving Doppler radars in combination with acoustic sensors or arrays (Shi et al., 2011). Acoustic microphone arrays are used as a second sensor modality to detect acoustic emissions from moving targets. Radar and acoustic measurements are combined to reduce false alarms. Depending on the case, acoustic beam forming can be applied resulting in interference suppression (Vasquez et al., 2008). Advanced signal processing techniques, applied to the sensors' measurements, can combine asynchronous radar and acoustic data to improve accuracy and to reduce the false alarm ratio. Usually the aim is to develop

low cost, low power combination of sensors including a Doppler CW radar at microwave frequencies and acoustic dynamic microphones to detect moving targets and motions (Kyritsis, 2016).

The methodology of joint multi-sensor exploitation technologies can be expanded to include other type of sensors i.e. geophone / heartbeat or CO2 sensors. Thus, a combination of EM radar with acoustic or similar type of sensors and their data is foreseen that can enable detecting and tracking persons inside various kinds of vehicles. Configurable front ends can be explored, which can be shared by multi-channels, designed to interface with a variety of sensors suitable for human presence detection. The aim is to result in low cost, easy to use units that can provide a first-level detection event and that could be used under different conditions, in order to contribute to the wider goal of assisting and enhancing vehicles inspection in land borders.

3.5.8 Summary - Conclusion and comparison of technologies





- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

3.6 Analytics (BCAT)

The Intelligent Border Control Analytics Tool (BCAT) will evaluate the performance of iCROSS systems and discover key patterns in the data that would help quickly identify false acceptance or false rejection of travellers based on the data collected in the Pilot study. BCAT will use state of the art machine learning and statistical approaches on the outcomes of each iCROSS system once the border control procedure is completed and the decision on how to process the traveller is finalized. This will enable achieving the following goals:

- Evaluate the performance of each iCROSS system and its effectiveness to the human border control agent independently and when used in collaboration with other iCROSS systems.
- Discover key patterns in the data associated with either false accept or false rejects of travellers, which can be used for better decision making at border control.

3.6.1 State of the Art Analytical Approaches

In this section, state of the art technologies that can be used by BCAT are introduced. The selected algorithms are widely used in the literature or have been recently proposed and show promising results. An attempt has been made to have both algorithms that account for linear dependence among the variables and algorithms that are capable of identifying non-linear dependencies among variables. This increases the probability of identifying any relationships that may be present in the data that will be analysed by the BCAT.

3.6.2 Correlation Analysis

In correlation analysis, the interest is in identifying any statistical relationship between two random variables. Such analyses in BCAT can reveal correlations of the outcomes of the iCROSS systems so as to see which systems behave similarly (e.g. it might reveal that there is a correlation among the ADDS and the DAAT output, which can then lead in identifying that travellers found lying by the ADDS tend to also have unauthenticated documents). There are various approaches for identifying such relationships, and we will present some that are widely used.

3.6.3 Pearson's Correlation Coefficient

Pearson's Correlation Coefficient measures the degree of linear correlation between two variables. The returned correlation is in the range $[-1,1]$, with zero denoting no correlation among the variables, 1 a perfect increasing correlation (when there is an increase in the value one of the variables there is a linear increase in the value of the other variable as well), and -1 a perfect decreasing correlation. The measure for two random variables X and Y is calculated with the following formula:

$$\text{corr}(X, Y) = \frac{\text{cov}(X, Y)}{\sigma_X \sigma_Y}$$

where cov is the covariance and σ is the standard deviation.

3.6.3.1 Randomized Dependence Coefficient

The Randomized Dependence Coefficient (RDC) (Lopez-Paz et al., 2013) is a measure of non-linear dependence between random variables based on the Hirschfeld-Gebelein-Renyi Maximum Correlation Coefficient. It is invariant to monotonically increasing transformations and it is ranged to $[0,1]$, with zero indicating no correlation and one indicating a complete correlation among the two variables. The RDC process for the variables \mathbf{x} and \mathbf{y} drawn from a noisy circular pattern is shown in the following figure. The samples are used to estimate the copula, and then are mapped with randomly drawn non-linear functions. The RDC is the largest canonical correlation between these non-linear projections.

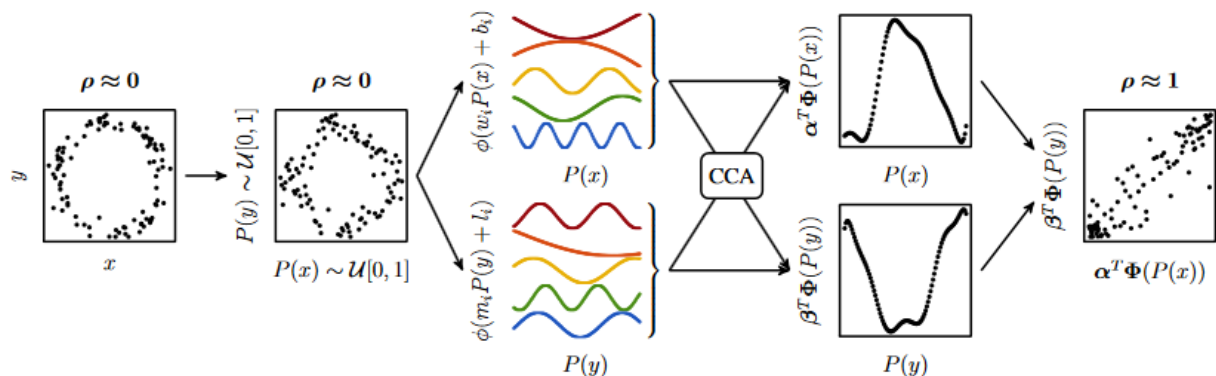


Figure 50 RDC computation

3.6.3.2 Dimensionality Reduction

Dimensionality Reduction can be used either for transforming the data into lower dimensions using the information of all available variables/features, or selecting a subset of the available features, so as to remove the ones that are redundant or irrelevant. This can be used for visualizing data in lower dimensions and for helping creating simpler models, which are less prone to overfitting.

3.6.3.3 Principle Component Analysis (PCA)

Principal component analysis (PCA) (Abdi and Williams, 2010) creates linearly uncorrelated variables (Principle Components) using orthogonal transformations. The resulting PCs are less than or equal to the number of the initial features. The largest variability in the data is explained by the first PC, then by the second and so on. PCA can be used for visualizing high dimensional data into lower dimension (e.g. 2 or 3) that can help in exploratory analysis. Additionally, it can be used for noise removal.

3.6.3.3.1 HSIC Lasso

The HSIC Lasso (Yamada et al., 2014), is a feature-wise kernelized Lasso approach. Since it is feature-wise, the kernel is applied on each feature vector, which enables the identification of non-linear dependence between a feature and the response variable. To identify features that are not redundant and are associated with the response variable the Hilbert-Schmidt Independence Criterion (HSIC) is used. The HSIC Lasso is given in the following form:

$$\min_{a \in \mathbb{R}^d} \frac{1}{2} \left\| \bar{L} - \sum_{k=1}^d a_k \bar{K}^{(k)} \right\|_{Frob}^2 + \lambda \|a\|_1, \text{ s.t. } a_1, \dots, a_d \geq 0$$

Where $\|\cdot\|_{Frob}^2$ is the Frobenius norm, $\bar{K}^{(k)}$ is the centered Gram matrix computed for the k-th feature and \bar{L} is the centered Gram matrix computed from the target variable. The algorithm returns the selected features with non-zero coefficients.

3.6.3.4 Clustering

Clustering is used for grouping data that have similarities together. The similarity between data is usually calculated using distance measures such as the Euclidean distance and the Hamming distance. Clustering can be used to group together travellers with similar patterns.

3.6.3.4.1 K-means

K-means (Hartigan and Wong, 1979) is a clustering algorithm that tries to partition data into k groups. The algorithm takes as input an MxN matrix and k which is the number of clusters that will be created. Initially the centers of the clusters are randomly assigned in the data space. At each iteration of the algorithm, the subjects are assigned to the cluster whose mean is closest to them. The similarity measure used is usually the Euclidean distance. Then the means of each cluster are updated so that they are the mean of the subjects that are assigned in that cluster. This procedure is repeated either for a pre-specified number of iterations or until convergence. A drawback of k-means is that k needs to be defined a-priori. An example of a k-means clustering on data using k=4 is shown in the following figure. Each colored dot represents the center of the cluster, calculated by k-means.

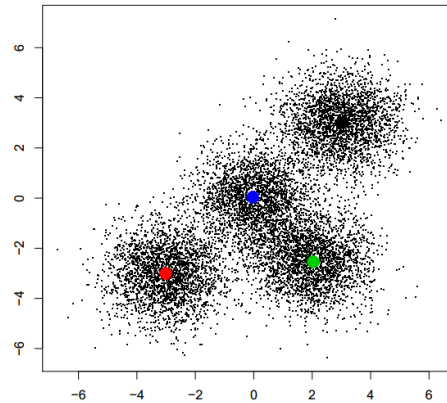


Figure 51. K-means clustering with $k=4$

3.6.3.4.2 Hierarchical Clustering

Hierarchical clustering techniques do not require from the user to a-priori define the number of clusters (Hastie et al., 2009). In hierarchical clustering there are mainly two strategies, the agglomerative and the divisive strategy. The difference between these two strategies is that the first follows a bottom up approach, whereas the second one follows a top down approach.

In agglomerative clustering, at each step the two closest clusters get merged together until only one cluster is left. There are several methods for deciding whether two clusters are close. One approach is to consider the distance between two clusters as the distance between the closest pair among the two clusters also known as the nearest neighbour technique. An alternative of this method is to consider the distance between the furthest pair of the two clusters, known as the furthest neighbour technique. A compromise between these two methods is to consider the average distance between the two groups.

An example of hierarchical clustering is shown in Figure 52. Four clusters were created as shown with different colors on the left dendrogram. The heatmap shows the different values of the data in each cluster so as to visualize their differences.

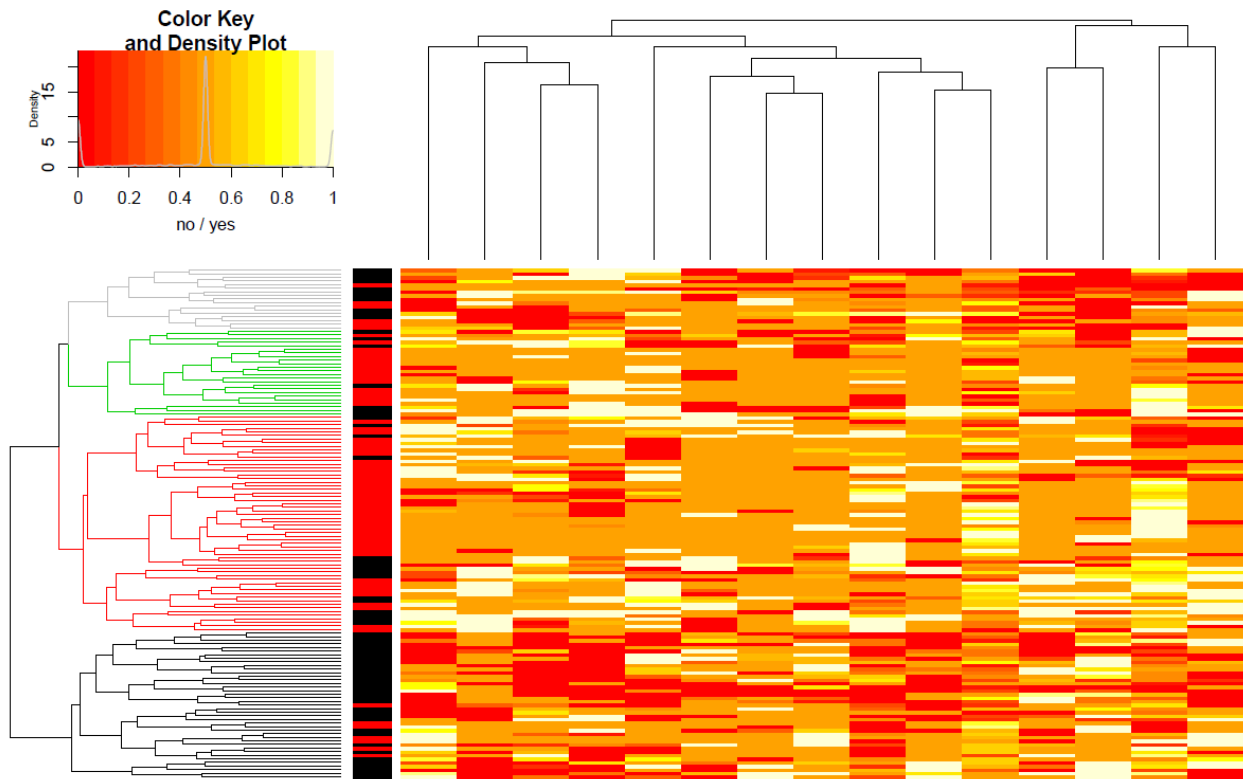


Figure 52 Hierarchical Clustering representation with a heatmap.

3.6.3.5 Classification

Classification algorithms try to predict the class of an instance using the knowledge they have from previously seen data. In BCAT classifiers will be used to aid the decision making in border control by modelling / identifying key patterns of travellers who should or should not pass into a country.

3.6.3.5.1 Random Forest

Random Forest (RF) (Breiman, 2001) is an ensemble of many de-correlated trees. Each tree is created using bootstrapping and the subjects not used are called the out of bag (OOB) samples, which are used for calculating the misclassification error. At each terminal node of the tree, m features out of p are randomly selected and the best feature out of them is used for further splitting the node. The trees are grown in full depth and no pruning is used. Majority voting is used for selecting the predicting class. The accuracy of the algorithm is calculated using the OOB error rate.

3.6.3.5.2 Support Vector Machines

Support Vector Machines (SVMs) (Cortes and Vapnik, 1995) are also known as maximum margin classifiers. This is due to the fact that they try to find the decision boundary that has the maximum margin among the data points of the classes in the dataset. The margin is defined as the perpendicular distance among the decision boundary and the closest of the data points as shown in the following figure.

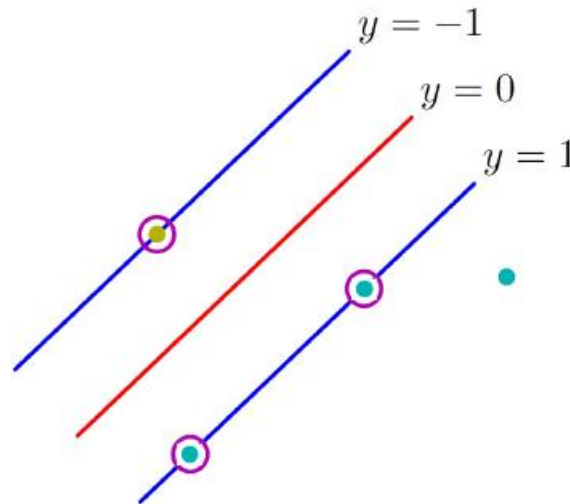


Figure 53 The decision boundary is $y=0$ whereas the margin is the perpendicular distance between the decision boundary and the closest data points of the two classes

To cope with the non-linearly separable data, kernel functions are used for projecting the data in higher dimensions and converting non-linearly separable problems to linearly separable.

3.6.4 Summary

Some of the state of the art algorithms for correlation analysis, dimensionality reduction, clustering and classification have been introduced. With such algorithms it is possible to identify common patterns among travelers of different categories and create models that aid the decision making in border control. So for increasing the power of BCAT, all of these analytical methods will be made available in the BCAT system.

3.7 Wireless Communication Networks

The scope of this Section is to introduce and investigate a set of basic deployment solutions of wireless network design for the efficient performance of the iCROSS platform. The section will begin with the actual components of wireless communication that suit the wireless access of iCROSS Platform perfectly. The presentation of the specific features of the activities of the agents will be presented afterwards and a proper connection with system performance at the various Layers of the Network Protocols Stack will be made. Finally, the performance measures identified by the overall analysis, necessary for dimensioning the iCROSS wireless network, will be shown.

3.7.1 Available Wireless Technologies for Radio Coverage and Connectivity

In this section, we present in brief the terrestrial and satellite communication technologies that can provide the radio connectivity in order to make the iCROSS platform functional and feasible. The wireless communication networks are either for backhaul connectivity or for the access networks. Here we will present them in the form of summary tables rather than specific details.

Regarding the choice and the advances under the framework of iCROSS, these will be conducted in WP6 and will be tailored to the needs of each of the pilot site. To this respect, the current SOTA of

the wireless networks solution, most suitable for the iCROSS implementation, are given in this section.

In

Table 11 we present briefly the technical details of the IEEE 802.11x standards (frequency of operation, channel bandwidth, data rate, modulation and the coverage for outdoor and indoor applications (Gosh, A. et al., 2005). In **Error! Reference source not found.**, the frequency ranges of the microwave links and their application are presented.

Table 11 802.11x standards

First of all 802.11 protocol	Frequency (GHz)	Bandwidth (MHz)	Data Rate (Mbit/s)	Modulation	Indoor/Outdoor	
					(m)	(m)
802.11	2.4	22	Up to 2	DSSS, FHSS	20	100
a	5	20	Up to 54	OFDM	35	120
					—	5km
b	2.4	22	Up to 11	DSSS	35	140
g	2.4	20	Up to 54	OFDM	38	140
n	2.4/5	20	Up to 65	MIMO-OFDM	70	250
		40	Up to 135		70	250
ac	5	20	Up to 86,7		35	
		40	Up to 200		35	
		80	Up to 390		35	
		160	Up to 780		35	
ad	60	2.160	Up to 6.912	OFDM, single carrier, low-power single carrier	60	100
ah	0.9					
aj	45/60					
ax	2.4/5			MIMO-OFDM		
ay	60	8000	Up to 100 Gbit/s	OFDM, single carrier	60	1000

Table 12 Microwave Links and Applications

Frequency Bands	Applications
1350-2690 MHz	Infrastructure, Radio Relays, Fixed Wireless Access (FWA)
3400-3600 MHz	Fixed Wireless Access
3600-4200 MHz	Infrastructure, Backhaul Networks
5925-6425 MHz	Infrastructure, Backhaul Networks, Radio Relays
6425-7125 MHz	Infrastructure, Backhaul Networks, Radio Relays
10-10.68 GHz	FWA, video links

10.7-11.7 GHz	Infrastructure, Backhaul Networks
12.75-13.25 GHz	Infrastructure, Radio Relays
14.25-14.5 GHz	Infrastructure, Radio Relays
14.5-15.35 GHz	Infrastructure, Radio Relays
17.7-19.7 GHz	Infrastructure, Radio Relays
22-23.6 GHz	Infrastructure, Radio Relays
24.5-26.5 GHz	Infrastructure, Radio Relays FWA
27.5-29.5 GHz	FWA, PMP links
37-39.5 GHz	Infrastructure, Radio Relays

Cellular networks have more than 30 years of history and today more than 7.5 billion mobile connections are active. There is a shift from ubiquitous voice coverage to the provision of mobile data at wired-like speeds (mobile internet speeds today exceed 10 Mbps) (3GPP, 2009; Poulakis, et al. 2014; Vassaki, et al. (2014) Papafragkakis, et al. 2015; Gotsis, et al., 2016). Mobile data speeds have increased by 1000x (kbps \rightarrow Mbps). Every new generation in cellular communications was marked by innovations in transceiver technologies and clear high-level objectives as seen in Table 13.

Table 13 Evolution of Cellular Networks

Evolution	Innovation(s)	Objective(s)
1G \rightarrow 2G	From Analogue to Digital Communications	Improve Voice Quality and Provide Basic Data (kbps) using GPRS
2G \rightarrow 3G	From Narrowband TDMA to W-CDMA and Turbo Coding	Improve Voice Capacity and Introduce THE killer app of Video-Call (FAIL). Instead it laid the foundations for mobile broadband data through HSPA
3G \rightarrow 4G	From W-CDMA to OFDMA and MIMO	Deliver the First Mobile Network designed and optimized for Data Provisions (tens of Mbps). No native support for voice (CS fallback, VoIP)

For each generation there is typical innovation cycle of 10 years for designing the system concept, technology components R&D, standardization, and pilot roll-outs. Multiple generations of cellular technology co-exist. 4G-LTE introduced in early 2010s and is the fastest growing system ever; Newer releases include 4G+ (LTE-A) and 4.5G (LTE-A Pro) Voice is provided by 2G/3G, Data primarily by 3G (various HSPA flavours) and 4G UE penetration is low. Moving now to Satellite Communications (Panagopoulos, 2015; Digital Video Broadcasting, 2009a; Digital Video Broadcasting, 2010; Digital Video Broadcasting, 2013; Digital Video Broadcasting, 2009b) Digital Video Broadcasting via Satellite standard was initially designed to offer digital video services but has proved to be a very attractive and successful protocol to provide multimedia applications via satellite. The return protocol known as DVB-Return Channel via Satellite (RCS) employs smaller spot beams while the forward link employs global beams. All the required procedures are controlled by the Network Control Centre (NCC) that is installed in the satellite gateway and one of its main tasks is reconfiguration of the burst time plan, when an atmospheric event occurs (Figure 54).

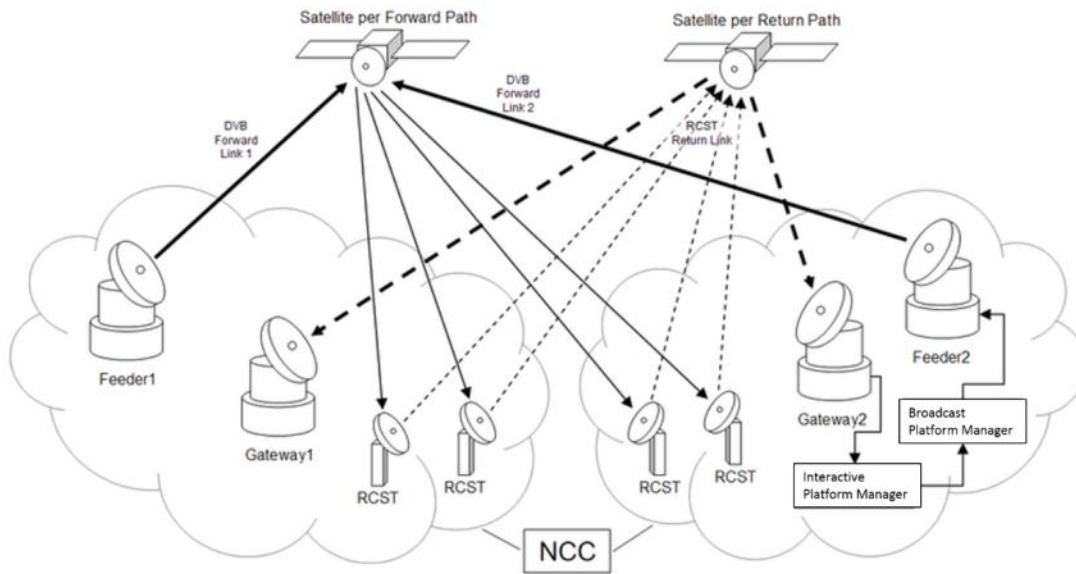


Figure 54 Architecture of DVB-S/S2 and DVB-RCS networks

DVB-S2 is the second-generation specification for satellite broadcasting – developed by the DVB (Digital Video Broadcasting) Project in 2003 and supported by European Space Agency. It benefits from more recent developments in channel coding (LDPC codes) combined with a variety of modulation formats (QPSK, 8PSK, 16APSK and 32APSK). When used for interactive applications, such as Internet browsing, it may implement Adaptive Coding & Modulation (ACM), thus optimizing the transmission parameters for each individual user, dependent on the satellite link conditions. The modes that are available are backwards compatible, allowing the operation of existing DVB-S set-top-boxes to continue working in the satellite users' premises. The DVB-S2 system has been designed for several satellite broadband applications: i) broadcast services for standard definition television and high definition television; ii) interactive services for consumer applications including access to the Internet; iii) professional applications and iv) data content distribution and Internet trunking. The technical details of the DVB-S and DVB-S2 are presented in Table 14. DVB-S2X is a very recent extension of the DVB-S2 satellite digital broadcasting standard. It was standardized in March 2014 as an optional extension of DVB-S2 standard. It will also become an ETSI standard. Efficiency gains up to 51% can be achieved with DVB-S2X, compared to DVB-S2. The most important transmission capability improvements are: higher modulation schemes (64/128/256APSK), smaller roll-off factors and generally improved filtering, making it possible to have smaller carrier spacing. In principle, DVB-S2X has been designed for very low SNR regions. Another standard for the return link is DVB-RCS2 that was approved in 2011 and in 2012 with its mobility extensions (DVB-RCS2+M) in order to support mobile/nomadic terminals and direct terminal-to-terminal (mesh) connectivity. Its features include handovers between satellite spot-beams, spread-spectrum features to meet regulatory constraints for mobile terminals, and continuous-carrier transmission for terminals with high traffic aggregation. It also includes link-layer forward error correction, used as a countermeasure against shadowing and blocking of the satellite link. The following modulation schemes are eligible in DVB-RCS2 BPSK, QPSK, 8PSK, 16QAM, Constant envelope – CPM and regarding channel coding 16-state PCCC turbo code (linear modulation) SCCC (CPM) exist.

Table 14 Technical Details of DVB-S-Standards

	DVB-S	DVB-S2
Input interface	Single transport stream (TS)	Multiple transport stream and generic stream encapsulation (GSE)
Modes	Constant coding & modulation	Variable coding & modulation and adaptive coding & modulation
FEC	Reed-Solomon (RS) 1/2, 2/3, 3/4, 5/6, 7/8	LDPC + BCH 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9, 9/10
Modulation	Single-carrier QPSK	Single-carrier QPSK with multiple streams
Modulation	BPSK, QPSK, 8PSK, 16QAM	BPSK, QPSK, 8PSK, 16APSK, 32APSK
Interleaving	Bit-interleaving	Bit-interleaving
Pilots	no	Pilot symbols

3.7.2 Network Dimensioning of the iCROSS Platform

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

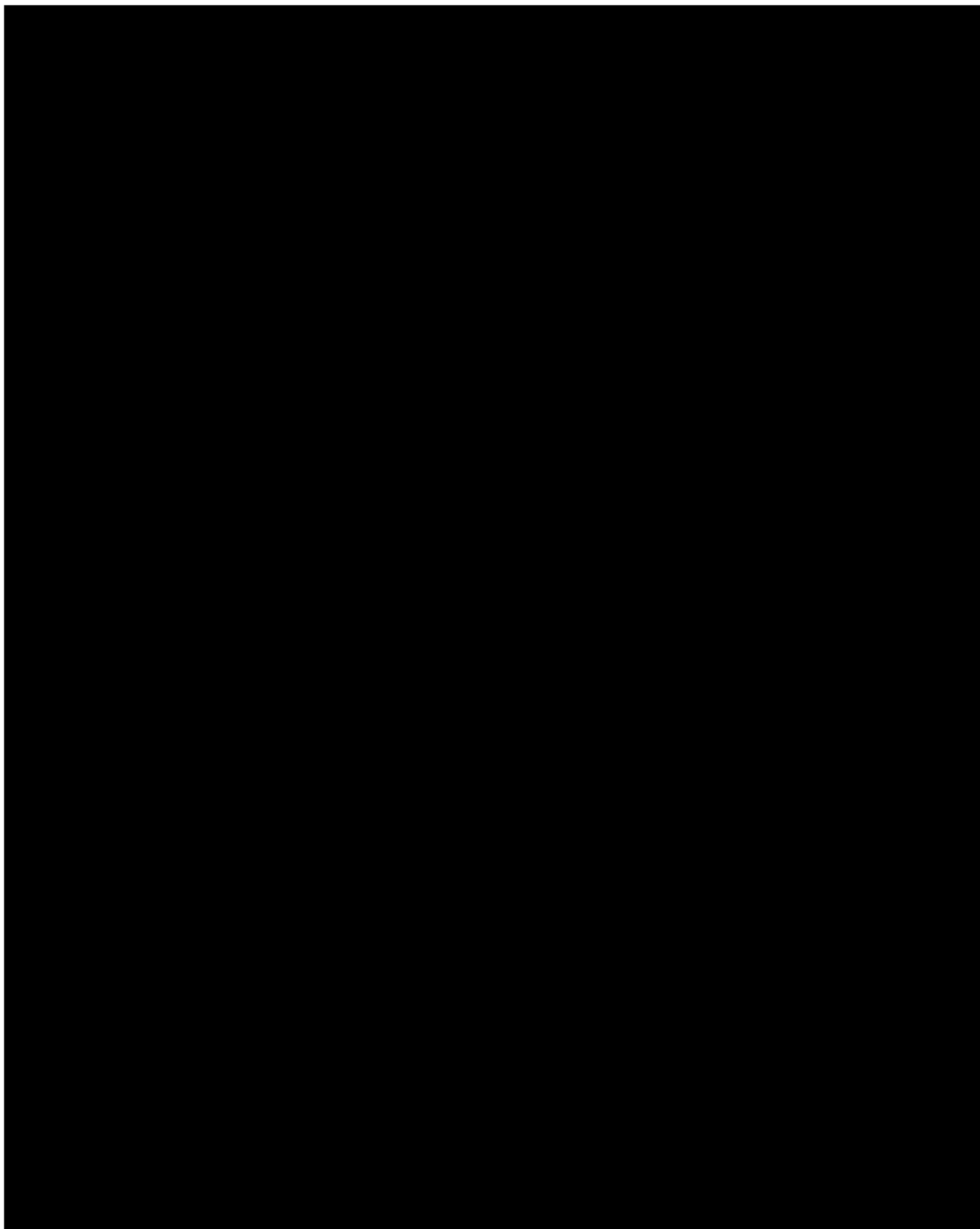
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





[REDACTED]

3.7.3 Performance measures for the iCROSS network design

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

3.7.4 Conclusions

In this section a combination of wireless components and deployment solutions was investigated, offering high connectivity as well as efficient performance to the iCROSS Platform. The specific traffic features of the envisioned iCROSS Platform were taken into account, concluding with respective performance measures that are appropriate for dimensioning purposes and fine-tuning of system parameters.

3.8 Related surveys

In the last few years, an increased focus on border security and management of goods and people moving across borders has been observed. The evolving international economic and security environments create a need for guidance in order to build border security capabilities, to integrate border security constructs and to increase protection at borders. Several surveys have been performed on behalf of governmental/state organizations in the last few years regarding how border management can be ideally addressed around the world. These surveys examine trends and challenges for a balanced and efficient approach for “Smart Borders” which are the foundation of safer, more standardized, and cost-effective borders.

According to a survey performed by Frontex (Frontex, 2015), border control systems can be divided into two types: (a) systems without enrolment based on the use of an electronic travel document and (b) systems based on pre-enrolment. The additional step with the pre-check process seems to be preferable as it reduces the time consumed for both the travellers and the border guards. Furthermore, the aforementioned survey emphasizes the indisputable necessity the cost-effectiveness of smart border control systems, namely to be implemented to allow an increased rate of traveller checks in a given time at first-line control without necessarily having to increase the number of border guards (well-trained and motivated operators can further contribute to the effectiveness of the systems). Another considerable aspect is the deployment of a risk assessment methodology that needs to be carried out for every task in the border check process that is modified, in order to understand how a new functionality impacts on existing risks or created new ones, and thus react accordingly.

Governments, in particular, pursue a border security and management paradigm that can create safer, more standard and cost effective demarcations. A report from Deloitte (Deloitte, 2014), describes four principles on how governments can transform the way they secure and manage their borders. These principles are the following: a) make a safer border by employing risk based decision-making, b) improve standardization by normalizing data requirements and partnering across borders, c) increase cost savings by consolidating government functions at the border and d) innovate at the border by enabling the ecosystem to bring commercial and community solutions.

More specifically establishing common assessment criteria and mutual guidelines for identifying, segmenting, and addressing risk is necessary in order to drive risk-based resource allocation. In order to implement more effective border management, a holistic approach must be adopted that has the dual objective of facilitating the entry of frequent travellers to the EU and improving the monitoring of available information. Many countries focus on streamlining and fortifying border security operations, and as a result, border security becomes an integrated way of addressing national security. This perspective enables a critical holistic view of operations and opportunities to streamline inefficient travel security procedures. To that end, there is a critical need for traveller’s engagement in order to enhance border security (Deloitte, 2014).

Additionally, according to a recent fact sheet of the European Commission (European Commission - Fact Sheet, 2016), the recent deployments on smart borders should improve the quality and efficiency of border crossing processes. New technologies should help Member States deal with increasing traveller flows, without necessarily increasing the number of border guards, and to promote mobility between the Schengen zone and third countries in a secure environment. It is therefore necessary to work towards integrated solutions for improved accessibility to data for

border management and security, in full compliance with fundamental rights. The information systems, where necessary and feasible, should be interoperable. Moreover, in order to reduce border crossing time for third country nationals and workload for border guards, the European Commission proposes the automation of most data and information capturing steps as well as data verification. By using a pre-border check application, travellers can verify their identity, have their picture or video taken and answer a set of questions. As a second step, the traveller is guided to a border control lane where the border guard has received information from the security databases, the confirmation of the traveller's identity and the answers to the questions. The border guard may ask further questions before deciding to grant (or refuse) access to the Schengen area. The benefit for travellers is the automated preparation of the border check before they reach the border guard, whereas previously they would have been simply standing in line and waiting. The overall benefit for all travellers is that queues become shorter once a sufficient number of travellers go through pre-check. The advantage for border guards is that the automation of the procedure and that he/she can concentrate on assessing the individual's situation.

The Smart Boarder Coalition requested a report from Cubic Transportation Systems and UCSD regarding the improvement of control in the US-Mexico borders [4]. This research concluded to the following: The initial step in creating an integrated border crossing system is the implementation of a state of the art system that will provide processing, storage, monitoring capabilities as well as inputs from sensors (e.g. cameras, biometric devices). The access to the system is enabled through a user friendly GUI and the system should provide a private cloud or browser-based system and in the future allow additional entities to connect to the service. Regarding biometric data, an electronic pre-check procedure can be implemented that will require scanned copy of the passport and information about the private vehicle used for transportation. Smart phone applications as well as back-end algorithms can also be developed to collect and analyse the provided information. All the above should be run in real time, so the results are available by the time the traveller reaches the border officer. A "green light" result would allow the officer to let the traveller or car proceed without additional time-consuming interaction.

Various countries have instituted stricter border security measures in the past decade and they wish to improve their border flow strategies. Upon examination of the emerging solutions that arise from the above surveys, we summarise below the trends and challenges that deserve special consideration when constructing a long term vision for border security and management:

- utilize a pre-check procedure in order to reduce the subjective control and workload of human agents (Frontex, 2015), (European Commission - Fact Sheet, 2016),
- use of a cost effective smart automated border control system (increased rate of traveller checks for the same number of border guards) (Frontex, 2015),
- establish an integrated and dynamic, intelligence-driven, risk model (Frontex, 2015), (Deloitte, 2014),
- create uniformity and consistency in data requirements and information by using a holistic approach that combines all possible checks (Deloitte, 2014),
- consolidate functions at the border by fusing risk-based analytics (Deloitte, 2014),
- promote travellers' participation and engagement (Deloitte, 2014),
- improve accessibility to information for border management and security in full compliance with fundamental rights (European Commission - Fact Sheet, 2016),
- implement a state of the art holistic platform that will provide processing, storage, monitoring capabilities and take inputs from sensors (e.g. cameras, biometric devices) (Cubic and UCSD, 2015),

- implement smart phone applications for information processing and interaction of travellers with the border authorities (Cubic and UCSD, 2015),
- incorporate cloud based architecture (Cubic and UCSD, 2015),
- automate the document verification process and vehicle characteristics identification (Cubic and UCSD, 2015)
- overall increase the objective control and efficiency during the border control check procedure (Frontex, 2015; Deloitte, 2014; Cubic and UCSD, 2015; European Commission - Fact Sheet, 2016).

3.9 Related Research Projects

Over the last years, a main strategic goal of the European Commission is to ensure a secure society, a term that includes both the protection of freedom and the security of Europe and its citizens. The basic challenge aims to direct the research and innovation activities towards the need to protect EU citizens, societies and economies as well as the infrastructures and services, prosperity, political stability and wellbeing. Among others, some primary aims of the secure societies challenge are the following: to fight crime and terrorism ranging from new forensic tools, to protection against explosives and to improve border security (ranging from improved maritime border protection to supply chain security) and to support the Union's external security policies including conflict prevention and peace building.

Many research initiatives are currently focusing towards this direction, namely to improve border control security using novel procedures and ICT tools. In this section a survey, regarding research projects whose objectives are similar to those of iCROSS, is presented along with a comparative study of their outcomes in relation to the iCROSS expected results, regarding innovation and focus towards the secure societies challenge.

BODEGA – Proactive Enhancement of Human Performance in Border Control

The aim of the BODEGA project is to build an expertise at the European level about Human Factors at border lines in a way to enhance its efficiency without side effects to the end users (border control agents, border control managers, land travellers, air travellers and maritime travellers).

The main objectives of the project are to investigate and model human factors in border control, to provide innovative socio-technical solutions for enhancing border guards' performance of critical tasks, support border management decision-making, optimize travellers' border crossing experience and develop a PROPER toolbox which integrates the solutions for easy adoption of the BODEGA's results by stakeholders in border control. PROPER toolbox will integrate ethical and societal dimensions to enable effectiveness and harmonisation across Europe regarding border control (Bodega-project.eu, 2016).

C-BORD – Effective Container Inspection at BORDER Control Points

The mission of C-BORD is to develop and test comprehensive, cost-effective solutions for the generalized inspection of container and large-volume freight in order to protect EU borders, coping with a large range of container non-intrusive inspection (NII) targets, including explosives, chemical warfare agents, illicit drugs, tobacco, stowaways and Special Nuclear Material (SNM).

Because freight containers are a potential means for smuggling, drug trafficking, and transport of dangerous or illicit substances the efficient NII (non-intrusive inspection) of containerized freight is critical to trade and society. The C-BORD goal is to increase the interdiction of illicit or dangerous

material in containerized freight and deliver new capabilities against critical operational requirements and constraints such as: increased throughput of containers per time unit, reduced need for costly, time-consuming and dangerous manual container inspections, lower false negative and false positive alarm ratios and operationally significant health and safety, logistics, cost and benefits issues.

C-BORD will test the new technologies through live field trials, in three use cases under real conditions at different border control points. More specifically the use cases aim to give a proof of capability regarding three different scenarios: Fully Automated Seaport Integration in Rotterdam port, a Rapidly Relocatable Checkpoint for Ports Integration in Gdansk port and Mobile Checkpoints Integration in Hungarian land border. A C-BORD Toolbox and Framework will help customs analyze needs for container NII, design integrated NII solutions, optimize the interdiction chain, and provide a systemic response to key functional, practical, logistical, safety and financial questions to support deployment (Cbord-h2020.eu, 2016).

FASTPASS – A Harmonized, Modular Reference System for all European Automated Border Crossing Points

FASTPASS is an integrated project designed to establish and demonstrate a harmonized, modular approach for Automated Border Control (ABC) gates.

Border control has to comply with very different kinds of demands: privacy-compliant, quick, accessible and easy to use border crossing process for the travelers, and secure, precise, highly reliable systems able to detect several kind of threats by border crossing for the border guards. Therefore, FASTPASS aims to develop an innovative solution centered on the end-users requirements, respecting the Data Protection concerns and innovating technologies for more efficiency. The final system will be tested at three type of borders: air (Vienna Airport, Austria), land (Moravita's border crossing point, Romania) and sea (Greece) to assess its transferability to the market.

The project's end-users are both travellers and border guards and they will evaluate, customize and adapt the solution depending on their requirements. FASTPASS focuses its efforts on four main areas: New technologies to enhance the security and the efficiency at border crossing, harmonization of the user experience during border control, modularity by incorporating three scenarios for each kind of border (land, sea, air) and proposing a solution adapted to their particular requirements and usability through the implementation of a border guard/ user interface (Fastpass-project.eu, 2016).

ABC4EU – Automated Border Control Gates for Europe

ABC4EU identifies the requirements for an integrated, interoperable Automated Border Control (ABC) system, taking into account the future needs derived from the Smart Border, other EU and national initiatives, and also paying very special attention to citizens' rights, privacy and other related ethical aspects. ABC4EU focuses in the need for harmonization in the design and operational features of ABC Gates, considering specially the full exploitation of the EU second-generation passports and other accepted travel documents.

The aim of ABC4EU is to make border checks more flexible and user-friendly for passengers by harmonizing the functionalities of border check automation. ABC gates facilitate more fluent travelling by shortening queuing time and affect many functionalities such as biometrics, gate design and the border check process itself. One of the main objectives of the project is to update and

integrate current ABC systems and extend their use to future e-Passports. Simultaneously, states can fight cross-border crime and illegal migration more efficiently, and provide a higher level of internal security, i.e. uniform across Europe. The system will also benefit different stakeholders, such as transport operators, as the increasing flow of travellers will be handled efficiently (Abc4eu.com, 2016).

MOBILEPASS – A Secure, Modular and Distributed Mobile Border Control Solution for European Land Border Crossing Points

MOBILEPASS focuses on research and development towards technologically advanced mobile equipment at land border crossing points. The project takes into consideration the fact that travellers request a minimum delay and a convenient, non-intrusive border crossing, while border guards must fulfil their obligation to secure the EU's borders against illegal immigration, terrorism, crime and other threats. As a result, the MOBILEPASS development process addresses both requirements, namely to keep security at the highest level while increasing the speed and the comfort for all legitimate travellers at land border crossing points. Aspects of a fast border crossing are the following: a reliable and convenient capture of biometric and passport data, dependable, secure wireless data transfer and modular mobile equipment optimized to the border control workflow.

Improved traveller identification technologies, such as contactless fingerprint capture and advanced mobile facial capture are expected to increase the security, minimize spoofing and evasion, while making the control less cumbersome for passengers. A system evaluation and demonstration will be done in two different EU member states (Romania and Spain). Compliance with European societal values and citizens' rights is central to the acceptance of the developed technologies, and will accompany the development throughout the project (Mobilepass-project.eu, 2016).

EFFISEC – EFFicient Integrated SECurity Checkpoints

EFFISEC delivers to border authorities more efficient technological equipment for identity and luggage control of pedestrians and travellers inside vehicles, at land and maritime checkpoints, while maintaining or improving the flow of people crossing borders and improving work conditions of border inspectors, with more powerful capabilities, less repetitive tasks, and more ergonomic equipment.

The main EFFISEC objectives are the enhancement of security and efficiency of land and maritime checkpoints through technology, the improvement of the working conditions for border inspectors and the increase of the flow of people crossing the border. Enhancing security and efficiency through technology includes the application of biometrics for identity checks on travel documents, luggage checks for dangerous and/or forbidden goods, and vehicle control including detection of stolen vehicles. Improving the working conditions for border inspectors includes application of ergonomic tools and enhancing the use of border inspectors' knowhow. With respect to increasing the flow of people across land and sea borders, fast processing is required, of both pedestrians and passengers within vehicles (Effisec.reading.ac.uk, 2016).

FIDELITY – Fast and trustworthy Identity Delivery and check with e-Passports leveraging Traveller privacy

Significant efforts have been invested to strengthen border ID checks with biometric travel documents embedding electronic chips (e-Passport). However, problems appeared regarding fraud in the e-Passport issuing process, including personal data leaks, difficulties in certificate

management, and shortcomings in convenience, speed and efficiency of ID checks, including the access to various remote databases. FIDELITY is a multi-disciplinary initiative, which aims to analyze shortcomings and vulnerabilities in the whole e-Passport life cycle, and develop technical solutions and recommendations to overcome them. The project will demonstrate privacy enhanced solutions to secure issuing processes, improved e-Passport security and usability, and improved management for lost or stolen passports. FIDELITY aims to provide more reliable ID checks, hence hinder criminal movements, and ease implementation of E/E records (Fidelity-project.eu, 2016).

TABULA RASA – Trusted Biometrics under Spoofing Attacks

The TABULA RASA project analyses the weaknesses of biometric identification process software in scope of its vulnerability to spoofing, diminishing efficiency of biometric devices. The goal is to provide more resistant systems and standards for protection of biometric devices against spoofing. Therefore, one of its main goals is to address some of the issues of direct (spoofing) attacks to trusted biometric systems, as conventional biometric techniques (e.g. fingerprints and face) are vulnerable.

Direct attacks are performed by falsifying the biometric trait and then presenting this falsified information to the biometric system, one such example is to fool a fingerprint system by copying the fingerprint of another person and creating an artificial or gummy finger that can then be presented to the biometric system to gain access falsely. In particular, the TABULA RASA project aims to address the need for a draft set of standards to examine this problem, propose countermeasures such as combining biometric information from multiple sources and examine novel biometrics that may be inherently robust to direct attacks (Tabularasa-euproject.org, 2016).

PROTECT – Pervasive and User Focused BiomeTrics BordEr Project

The goal of the PROTECT project is an enhanced biometric-based person identification system that works robustly across a range of border crossing types and that has strong user-centric features. The system will be deployed in Automated Border Control (ABC) areas supporting border guards to facilitate smooth and non-intrusive rapid crossing by travellers based on deployment of the next generation of biometric identification detection methods. The ability for the system to process low-risk travelers efficiently, combined with increased levels of accuracy, security and privacy standards and enabling border guards to concentrate resources on higher-risk travellers, are central ambitions of the project. To achieve these goals, a multi-biometric enrollment and verification system is envisaged, taking into account current and next-generation e-Passport chips, mobile equipment and person identification ‘on the move’. Research will be undertaken into optimization of currently deployed biometric modalities, application of emerging biometrics (including contactless finger vein, speaker recognition and anthropometrics), multi-modal biometrics and counter-spoofing, for border control scenarios. An integral part of the project is collection and dissemination of new border-realistic biometric datasets, and systematic evaluation of the developed biometric methods including vulnerability and privacy assessment. The PROTECT project is strongly user-driven and a demonstration of the developed biometric system will be conducted at two different border crossing sites. Finally, the PROTECT project will make contributions to facilitating border crossing of bona-fide non-EU citizens as well as evolving standards in biometric systems (Cordis.europa.eu, 2016a).

ORIGINS – Recommendations for Reliable Breeder Documents Restoring e-Passport Confidence and Leveraging Extended Border Security

The project ORIGINS aims to study the security of the extended border and more particularly passport breeder document (e.g. birth certificate) security. The underlying idea of ORIGINS is to

improve the security and therefore to restore the confidence in the application process and issuance of e-passports, by filling the gaps in security of breeder documents. Indeed, while some assurance approaches have been implemented in a few countries, they remain insufficient to provide breeder documents in complete security and trustworthiness at a time when this is increasingly necessary (Origins-project.eu, 2016).

GLOBE - European Global Border Environment

The GLOBE project will provide a comprehensive framework in which an integrated global border management system must be developed. The project will take into account the current and future technological environment. Additionally, GLOBE's scope reaches even further by looking into other key aspects of border management beyond isolated technology, such as the legal and political environment, the social and economic impact of border problems and, more specifically, the impact on information management and integration. The proposal is founded on the conceptualisation of the end user's needs. These needs are well known by the partners of the consortium due to the hands-on experience that all companies have in the different border control areas. End users from several countries have participated in the conceptualization of the proposal to make sure it includes what they consider the most relevant issues in their areas of expertise Cordis.europa.eu, (2016b).

Table 17 illustrates how most of the abovementioned projects are compared, in terms of their focus and innovations with iCROSS.

Table 17 Comparison and Innovation and Focus on Existing Projects

✓: Related to (and to be considered by) iCROSS, ✗: iCROSS Innovation not covered

Project	Reduce Border Control Time	Use Cases	User / Social Engagement	Legal and Ethical Issues	Risk Analysis	Mobile Application	Deception Detection Tools	Biometric Analytics	Novel Verification Tools for Travel Documents	Vehicle control for hidden humans/illicit goods
BODEGA	✗	✓	✓	✓	✓	✓	✗	✗	✓	✗
C-BORD	✓	✓	✗	✗	✗	✗	✓	✗	✗	✓
FASTPASS	✓	✓	✗	✓	✗	✗	✗	✓	✓	✗
ABC4EU	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗
MOBILE-PASS	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗
EFFISEC	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓
FIDELITY	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗
TABULA RASA	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗
PROTECT	✓	✓	✓	✗	✗	✓	✗	✓	✓	✗
ORIGINS	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
GLOBE	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗

In Table 17 the most important research projects regarding border control security are compared based on innovations and provided services. As it is evident from Table 17, all existing projects

mainly focus on the solution of a particular problem (e.g. deception detection, vehicle control for hidden humans or goods, reduce time at the borders etc.) using several technologies.



3.10 Overall Conclusion of Current State of the Art

In the framework of Section 3, an extended description of the current State of the Art Technology was presented. Existing Border Control Platforms and IT solutions were examined along with the State of the Art of the main technological components of the iCROSS system. Existing commercial solutions, related literature and academic research were thoroughly reviewed while the achievements of related research projects were also identified for benchmarking.

This section identified and analysed important factors to be considered in the definition of the system requirements for the iCROSS solution; both in terms of features stemming from the different technologies offered by iCROSS partners and by existing solutions available in the market, as well as the new trends according to policy maker's surveys. These factors along with the comparison of technologies and the identification of technology gaps provide valuable results that will be used as inputs to the process of eliciting the requirements connected to the different tools and technologies offered by the iCROSS partners.

By this way, it is evident that the iCROSS project can provide significant added value by stimulating new research on the topic of land borders control incorporating a large innovation potential. Within the context of the aforementioned analyses, limitations of proprietary tools and technologies have been identified, while, what can be obtained and implemented within iCROSS has been examined.

All the above, will be correlated with the end-users requirements defined in the next sections of this report, to formulate a complete innovative system that will offer all requested and missing functionalities in the service of the land borders check procedures. This process of combining end-user requirements and technological capabilities will be more evident and substantial within the activities implemented in the Deliverable 2.2, where both the reference system architecture will be designed and the respective system specifications will be defined.

4 Requirements Capture and Analysis

4.1 Requirements Capture Methodology

[Redacted text block]

[Redacted text block]

[Redacted text block]

4.1.1 User Perspective

[Redacted text block]

[Redacted text block]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

I [REDACTED]

I [REDACTED]

I [REDACTED]

I [REDACTED]

I [REDACTED]

[illegible]

4.1.2 State-of-the-art Analysis

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

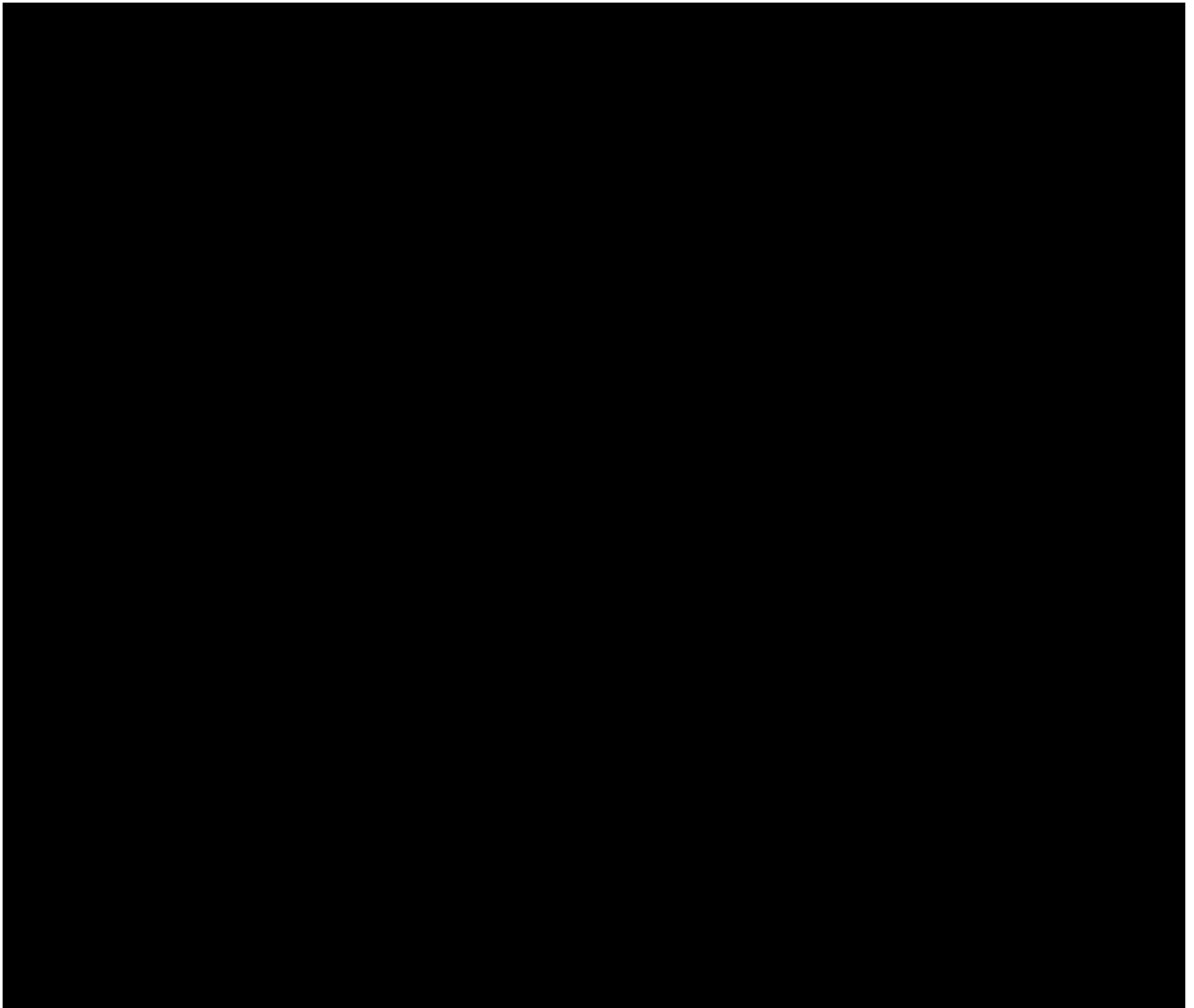
[REDACTED]

4.1.3 iCROSS system

[REDACTED]

[REDACTED]

[REDACTED]



4.2 Classification of requirements

[Redacted]

- [Redacted]
[Redacted]
[Redacted]
- [Redacted]
[Redacted]

[Redacted]
[Redacted]

[Redacted]

[Redacted]
[Redacted]

- (b) (7)(C), (b) (7)(D)
- | | 2019 | 2020 |
|---|------------|------------|
| ■ | [REDACTED] | [REDACTED] |
| ■ | [REDACTED] | [REDACTED] |
| ■ | [REDACTED] | [REDACTED] |

[illegible]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] [REDACTED]

4.3 Travellers Survey Analysis

4.3.1 Methodology for Traveller Closed Question Analysis

[REDACTED]

[REDACTED]

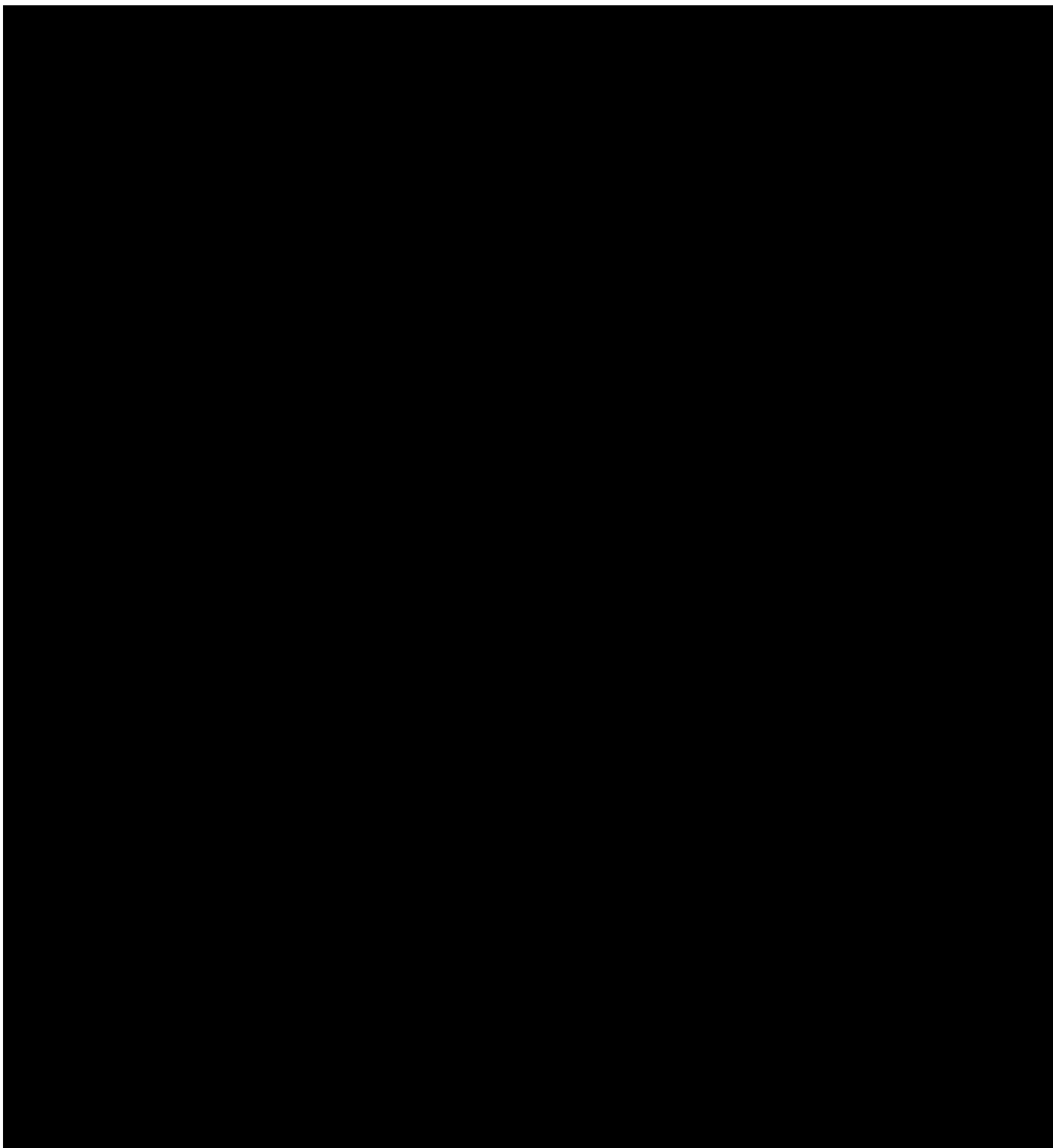
4.3.2 Results of Closed Question Analysis

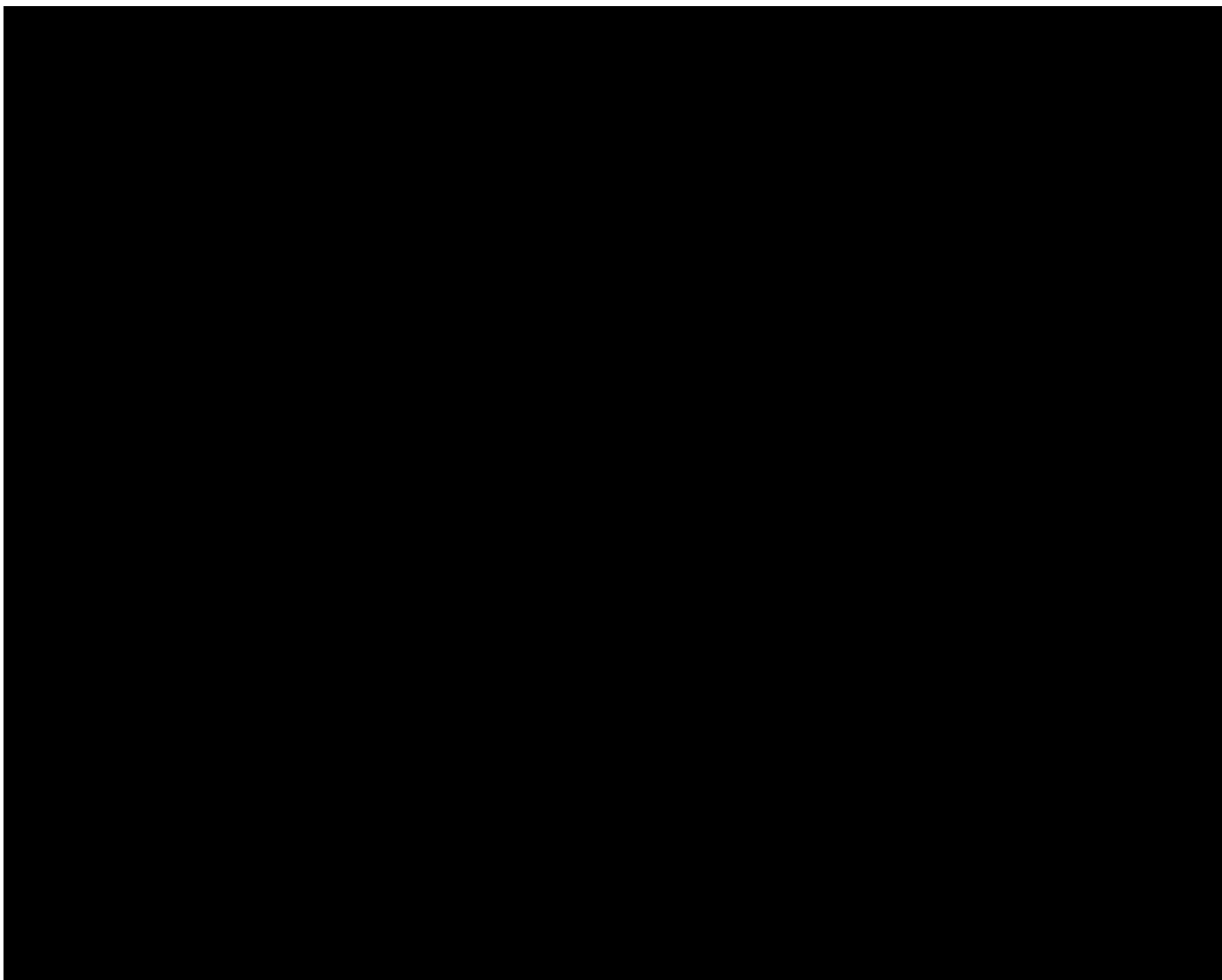
[REDACTED]

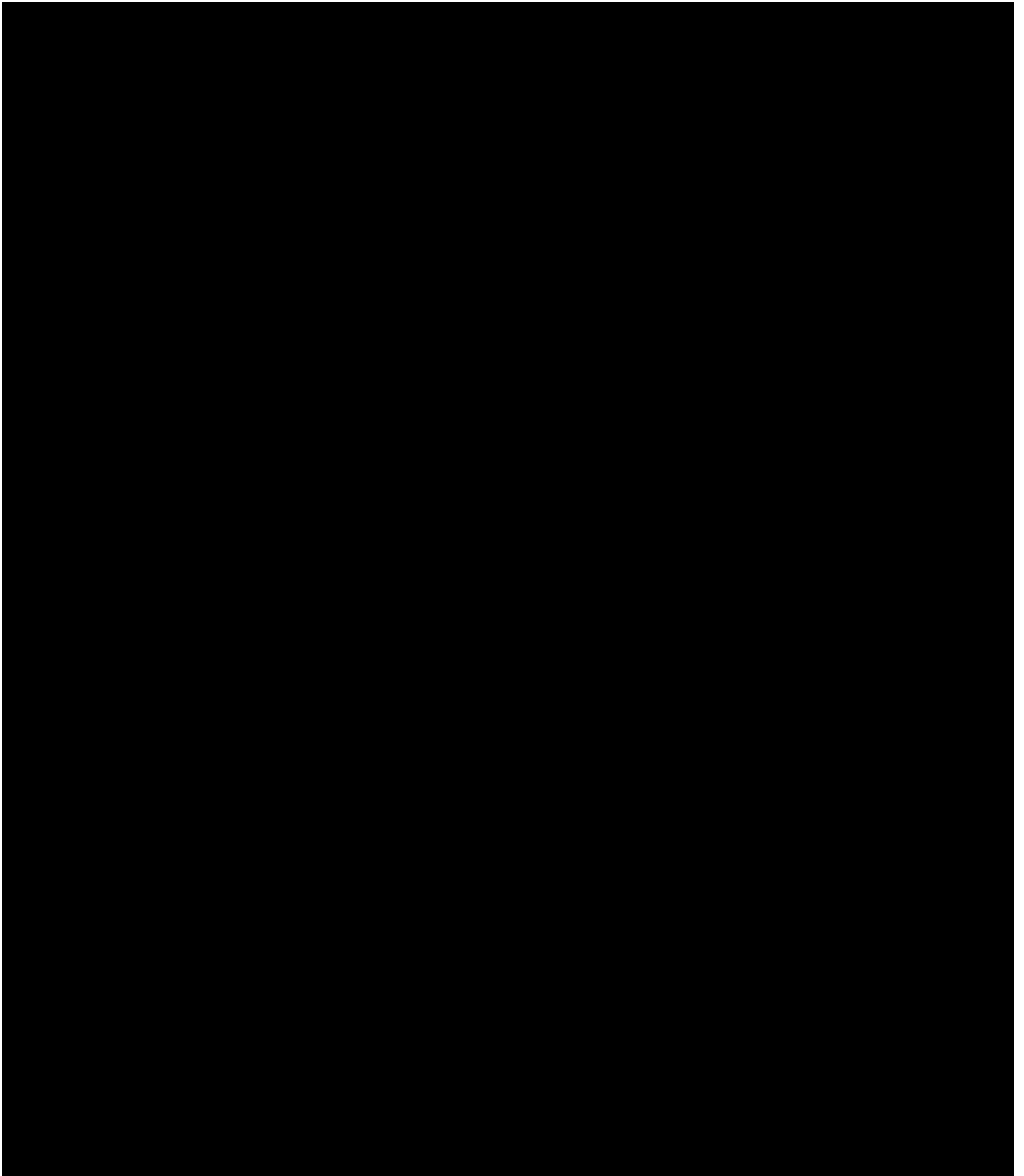
[REDACTED]

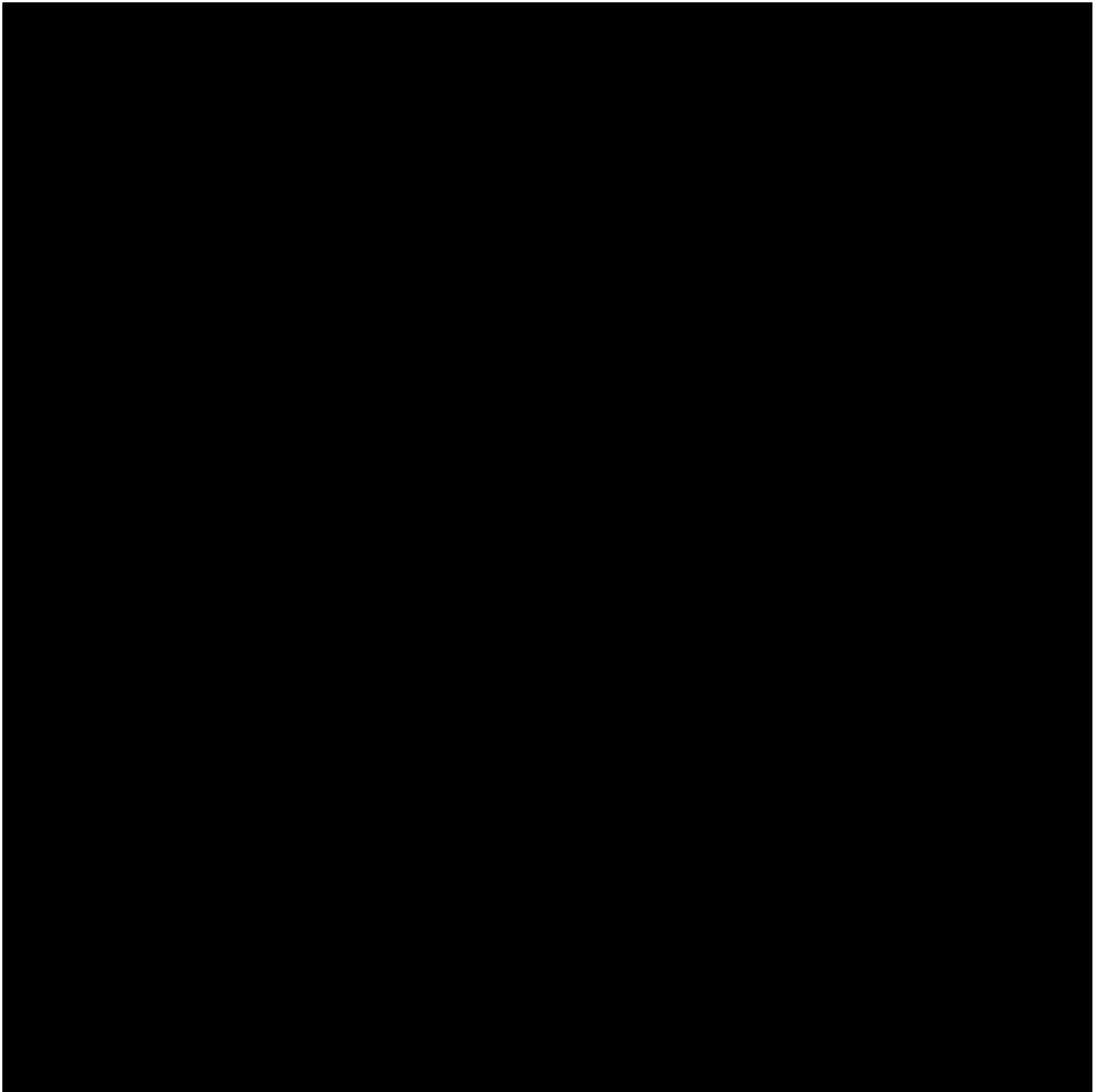
[REDACTED]

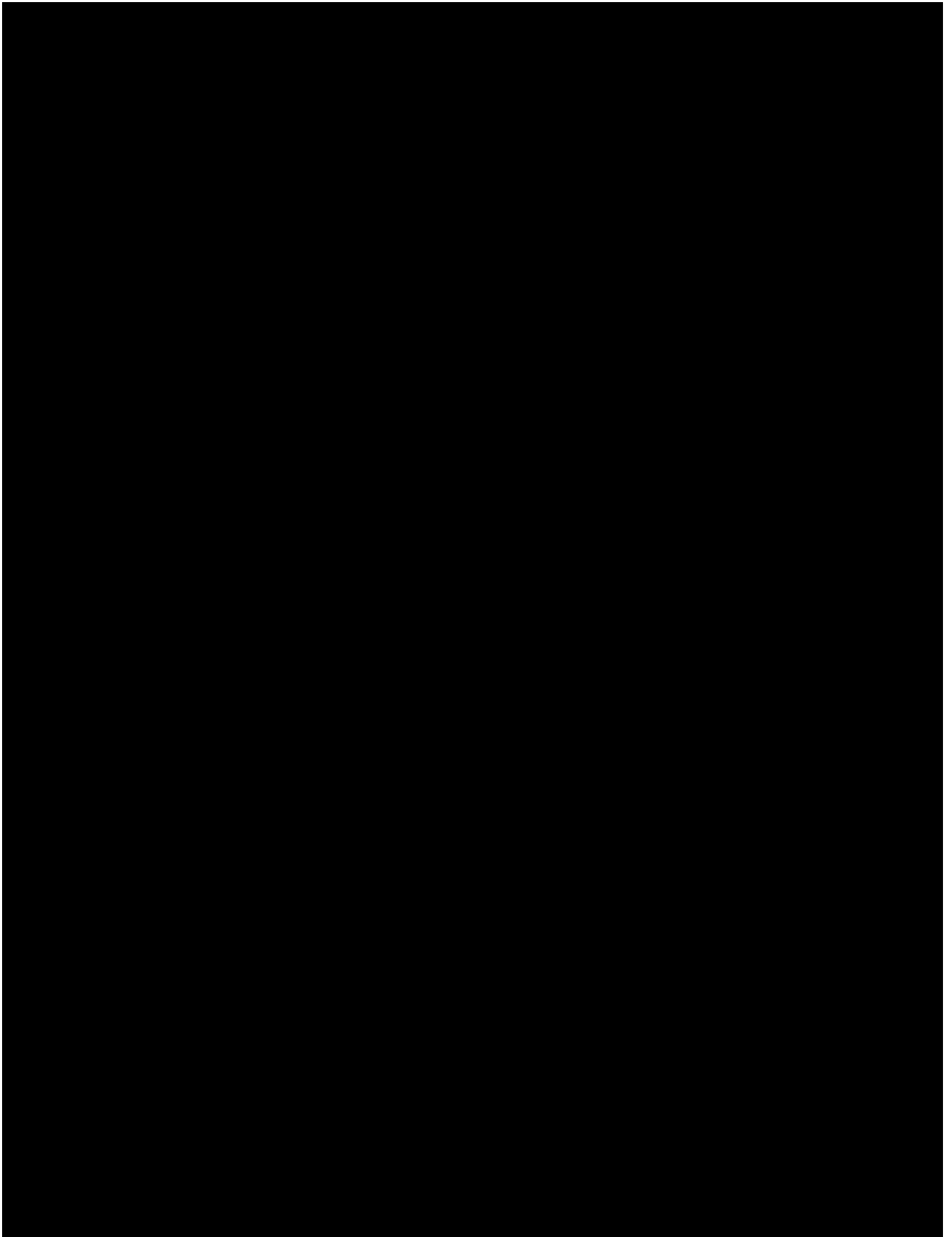
[REDACTED]

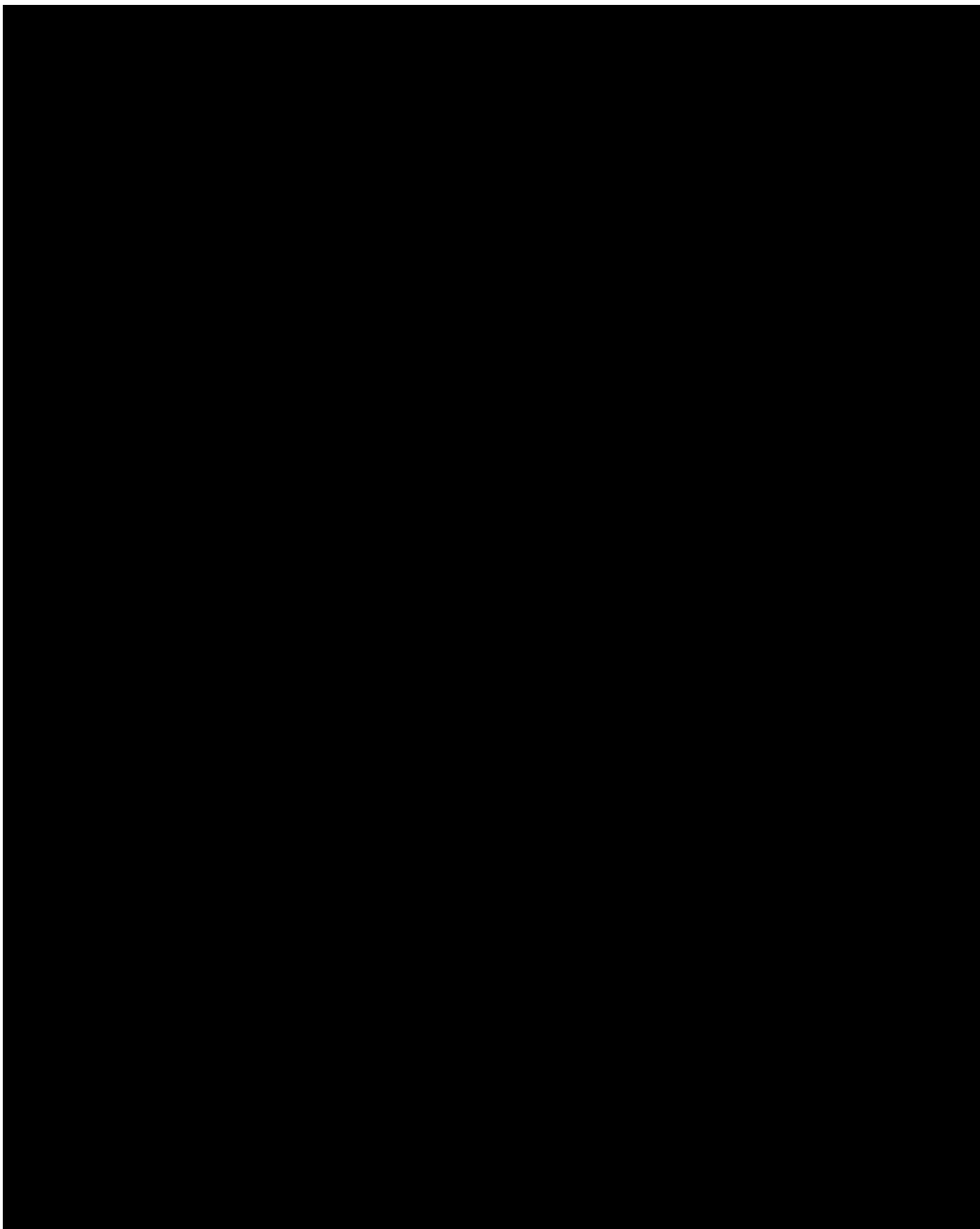


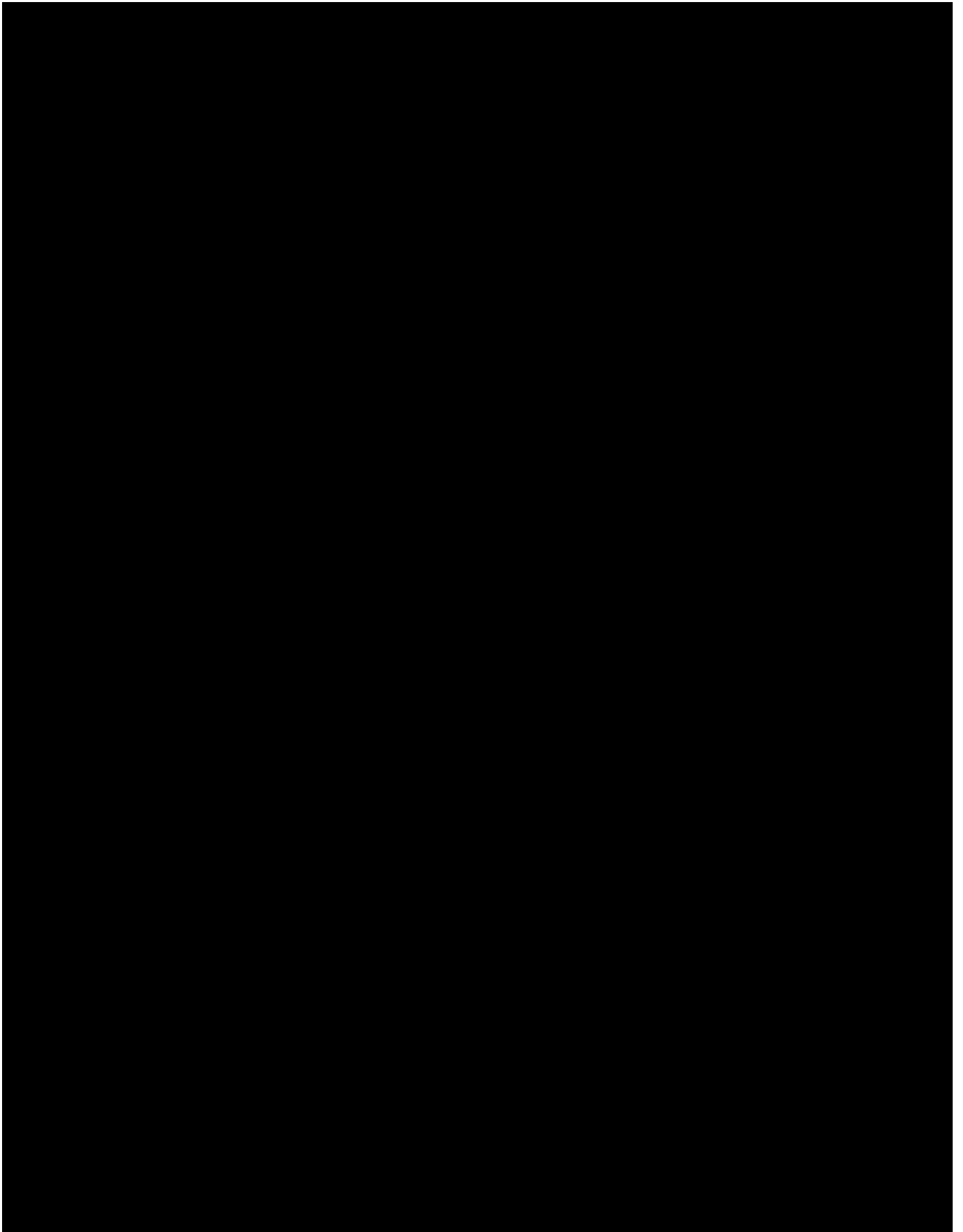


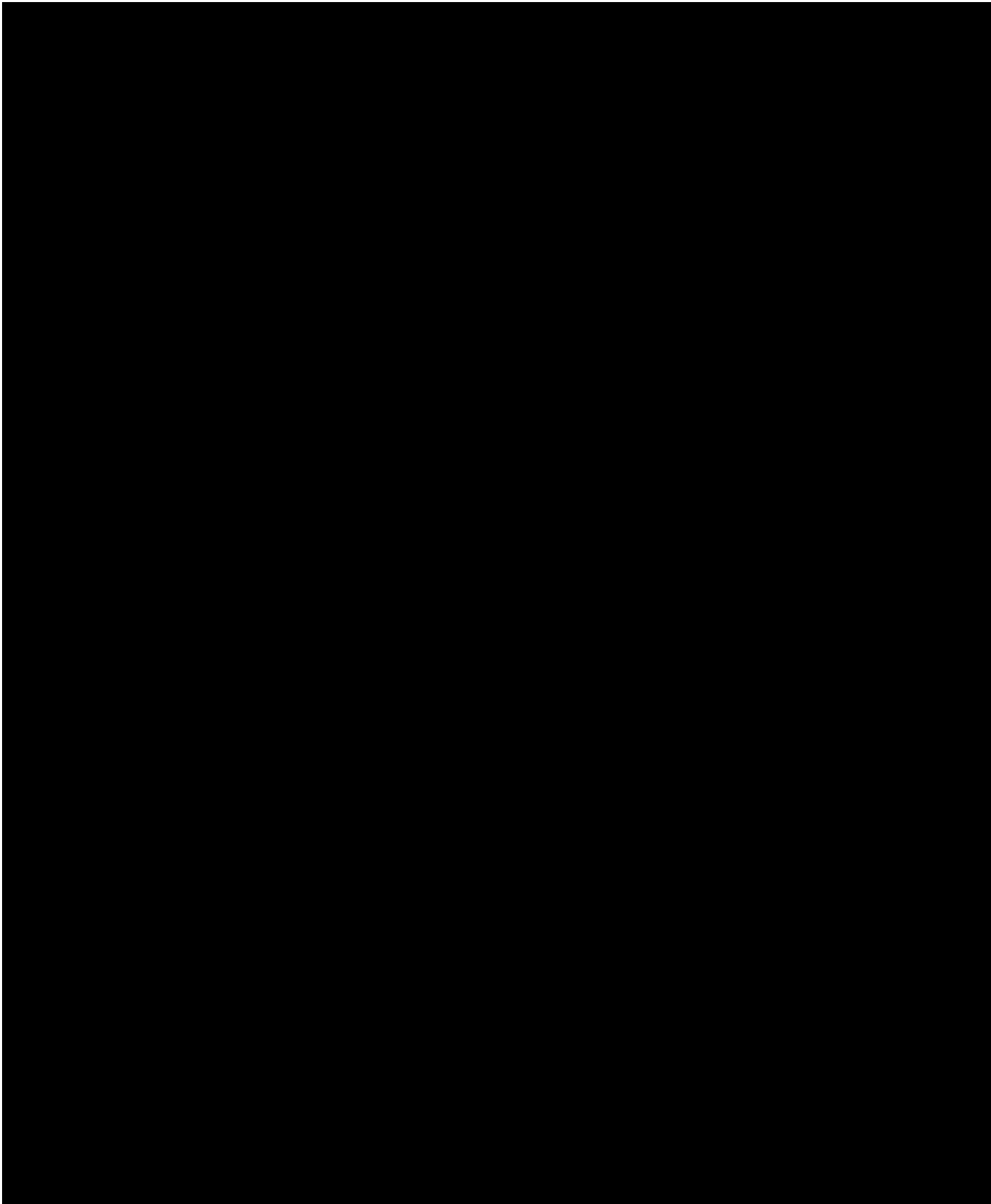












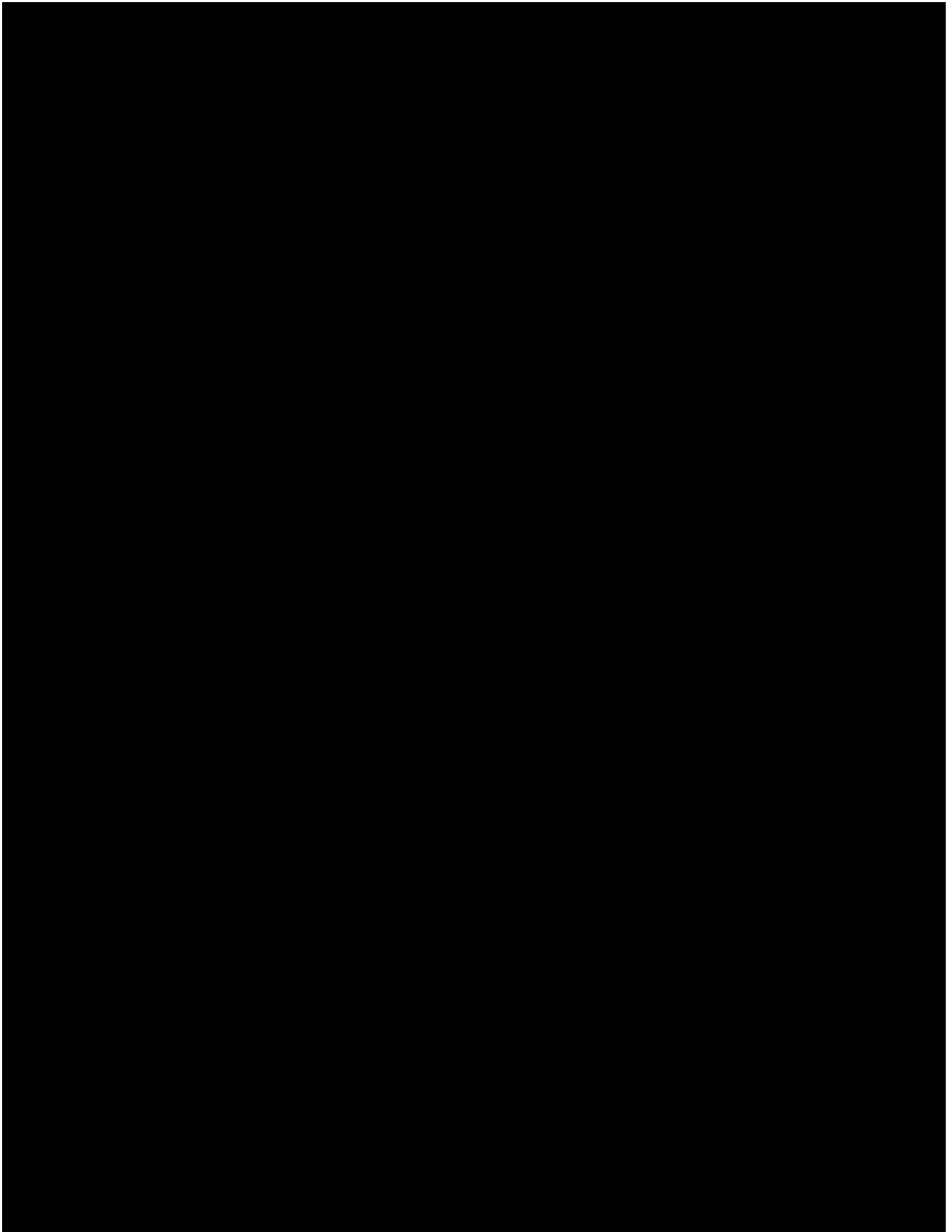
4.3.3 Methodology for Traveller Open Question Analysis

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

4.3.4 Results for Open Question Analysis

[REDACTED]



- [REDACTED]
 - [REDACTED]
- [REDACTED]
- [REDACTED]
 - [REDACTED]

[REDACTED]

- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]

- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- [REDACTED]
- [REDACTED]

4.3.5 Conclusions from Travellers Survey

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

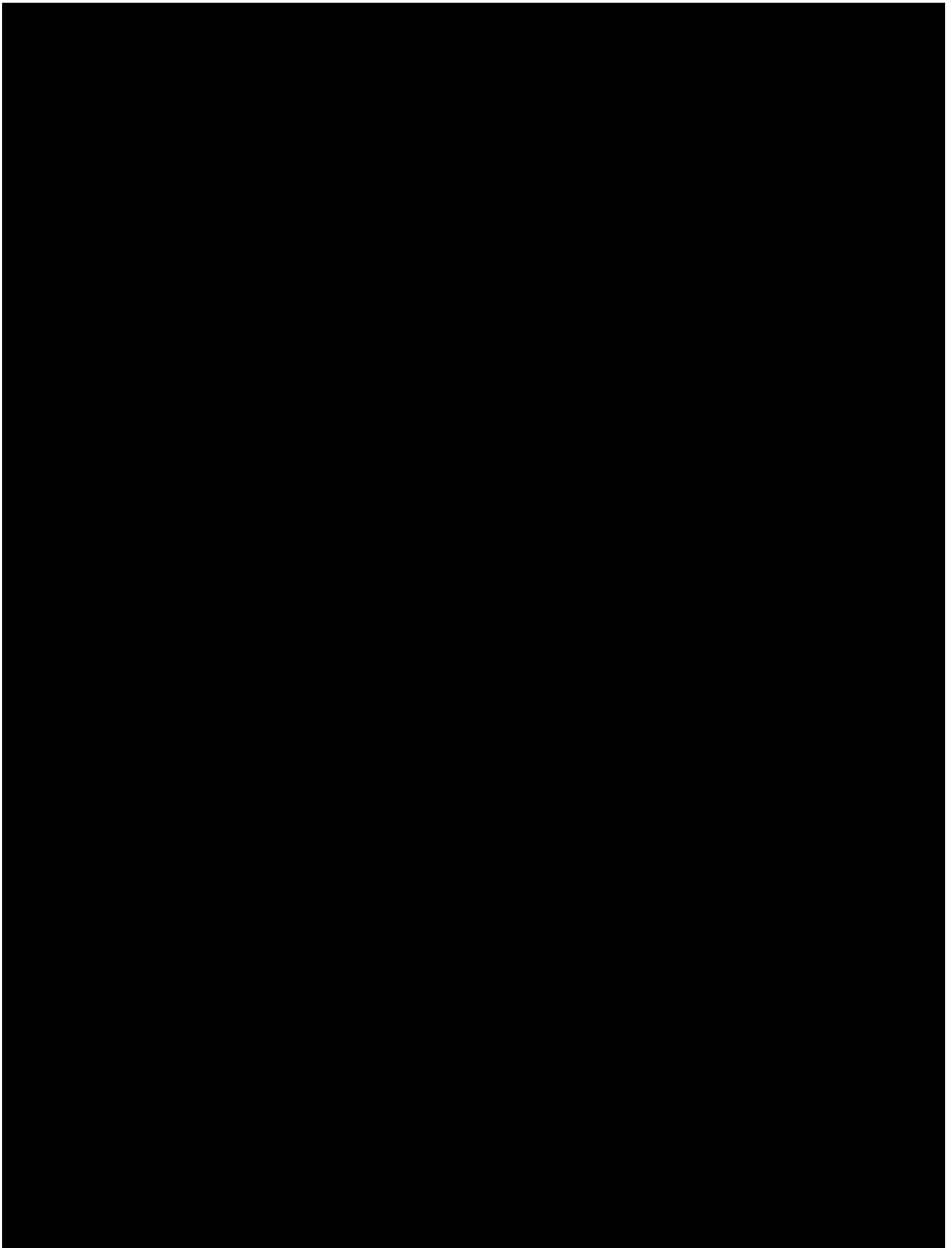
4.4 Stakeholder Interviews Analysis

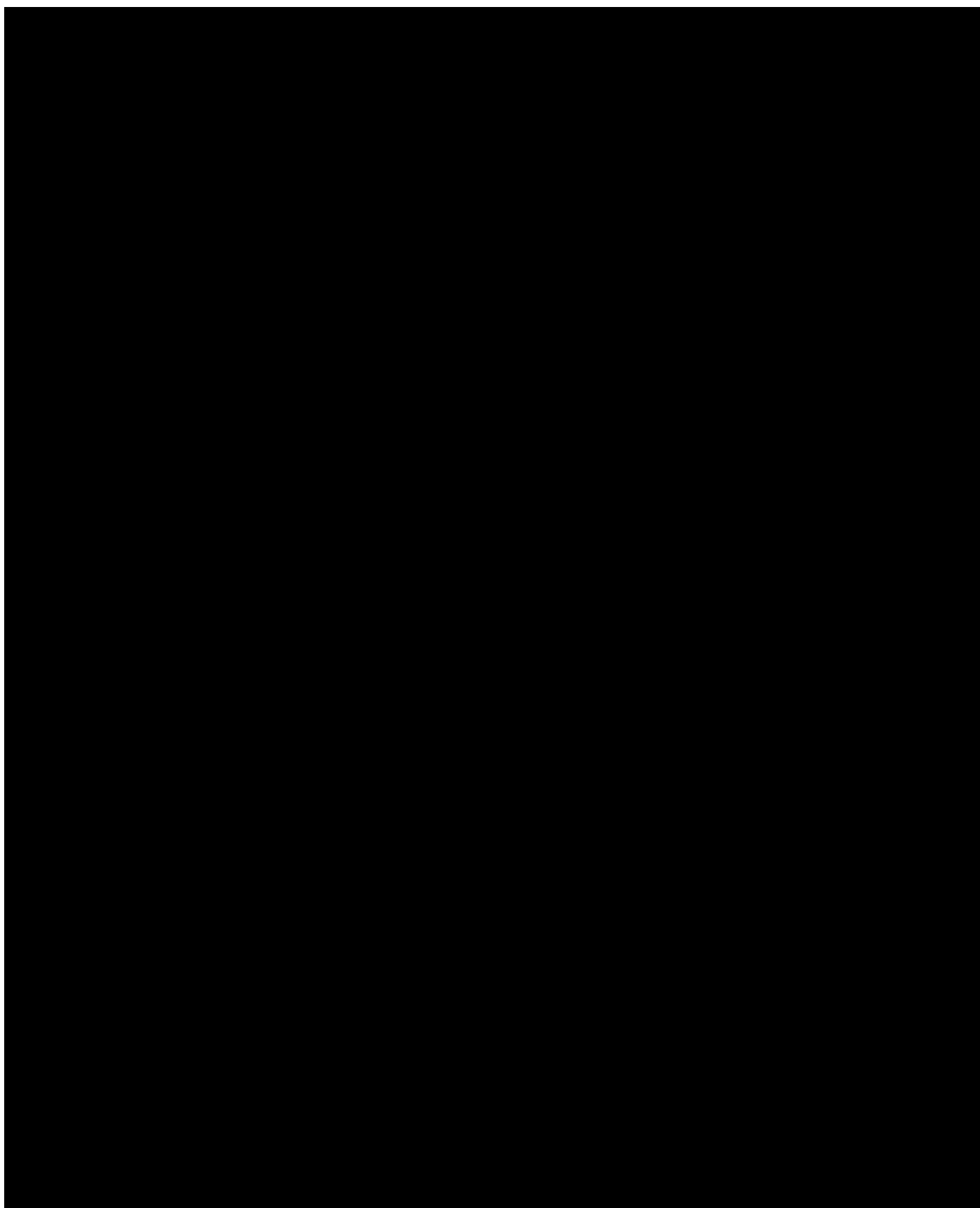
[REDACTED]

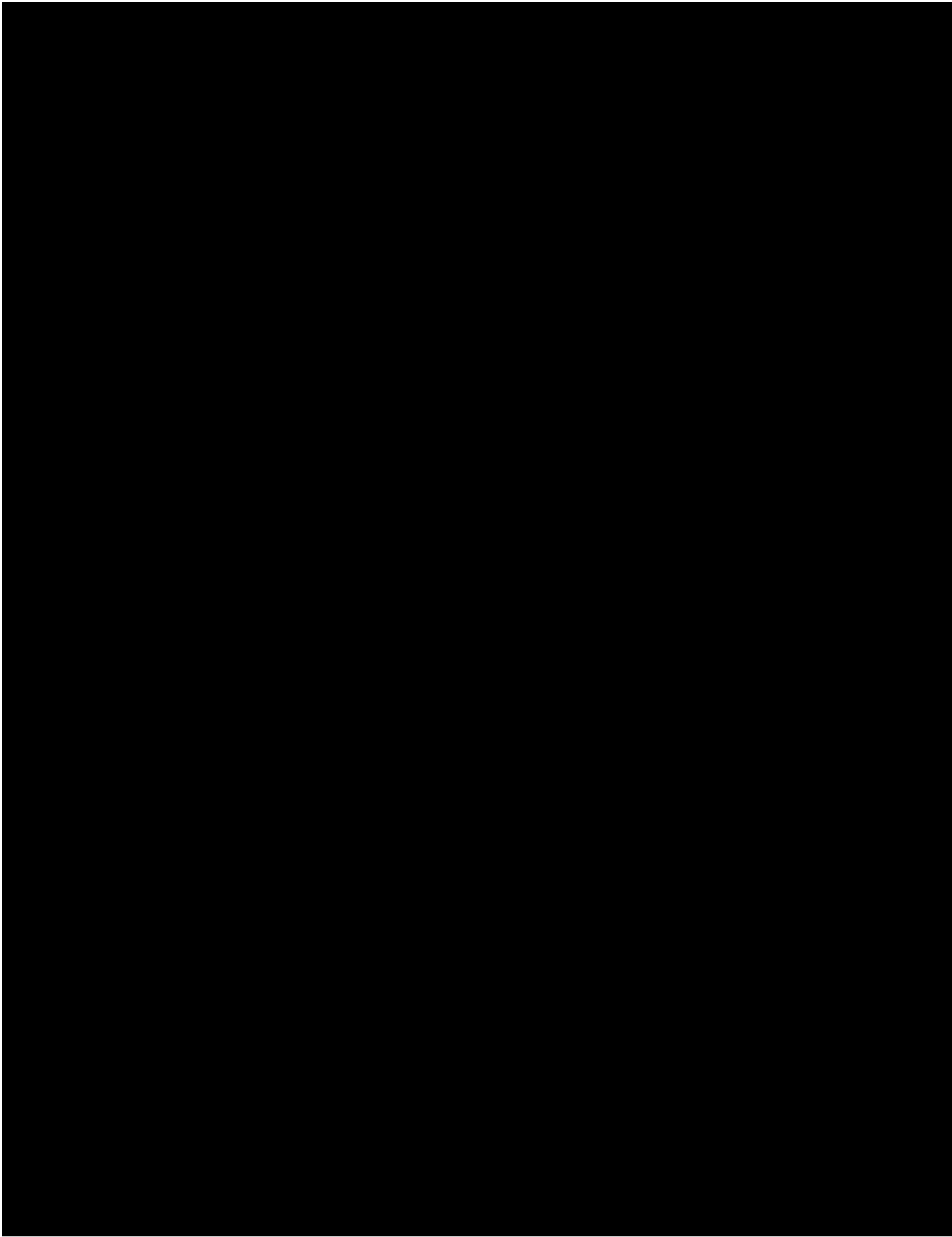
[REDACTED]

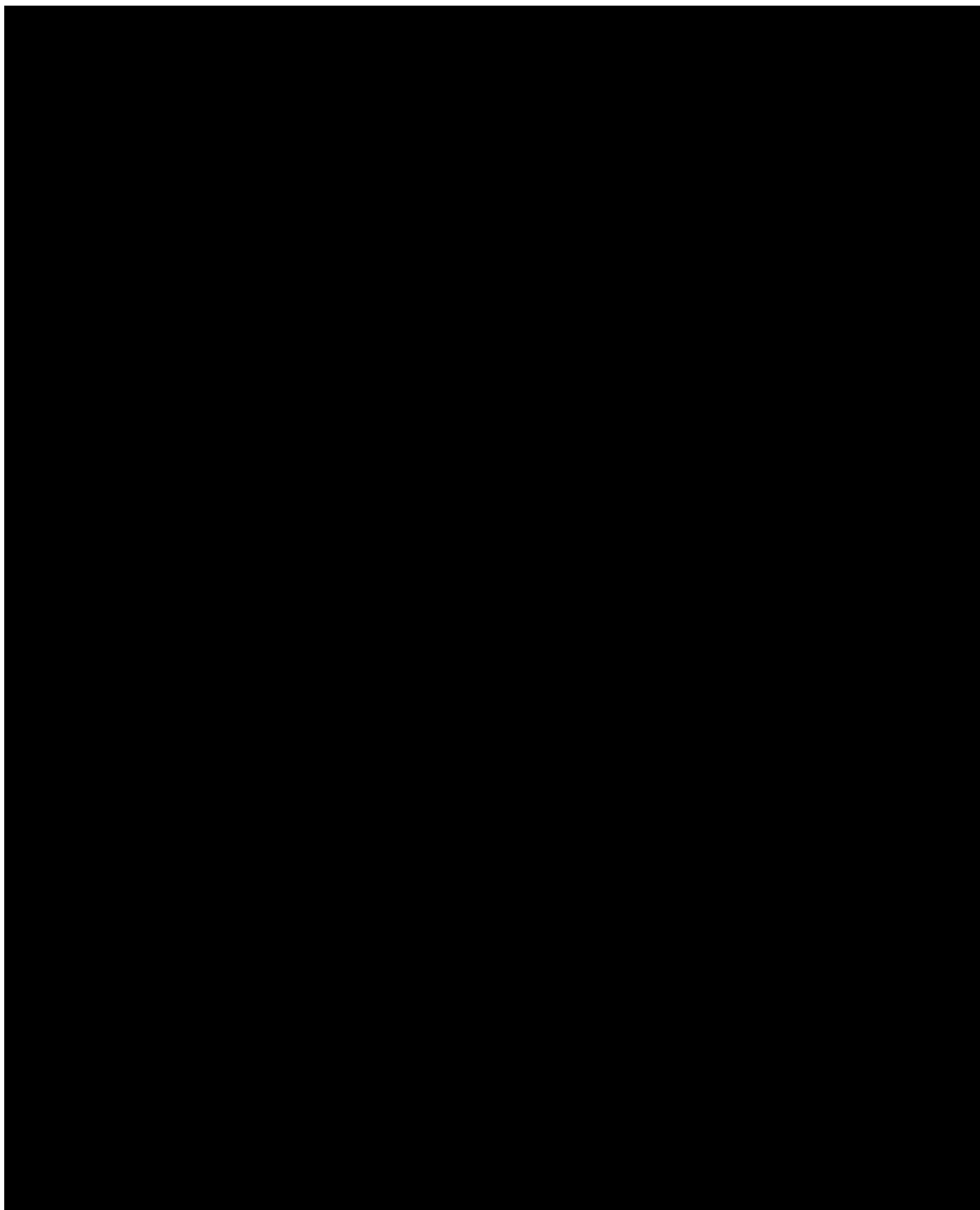
4.4.1 Analysis of Questions

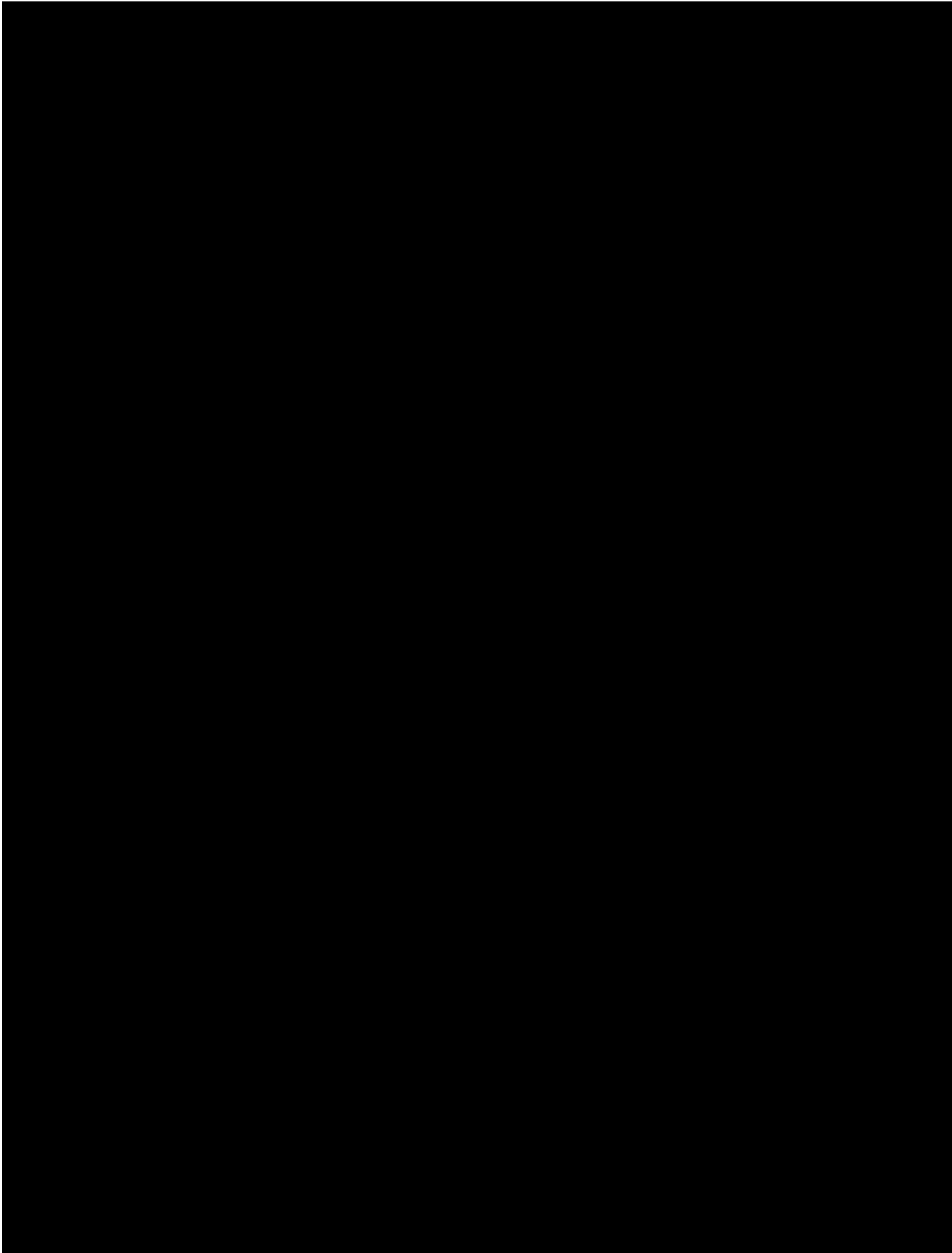
- [REDACTED]
- [REDACTED]
- [REDACTED]

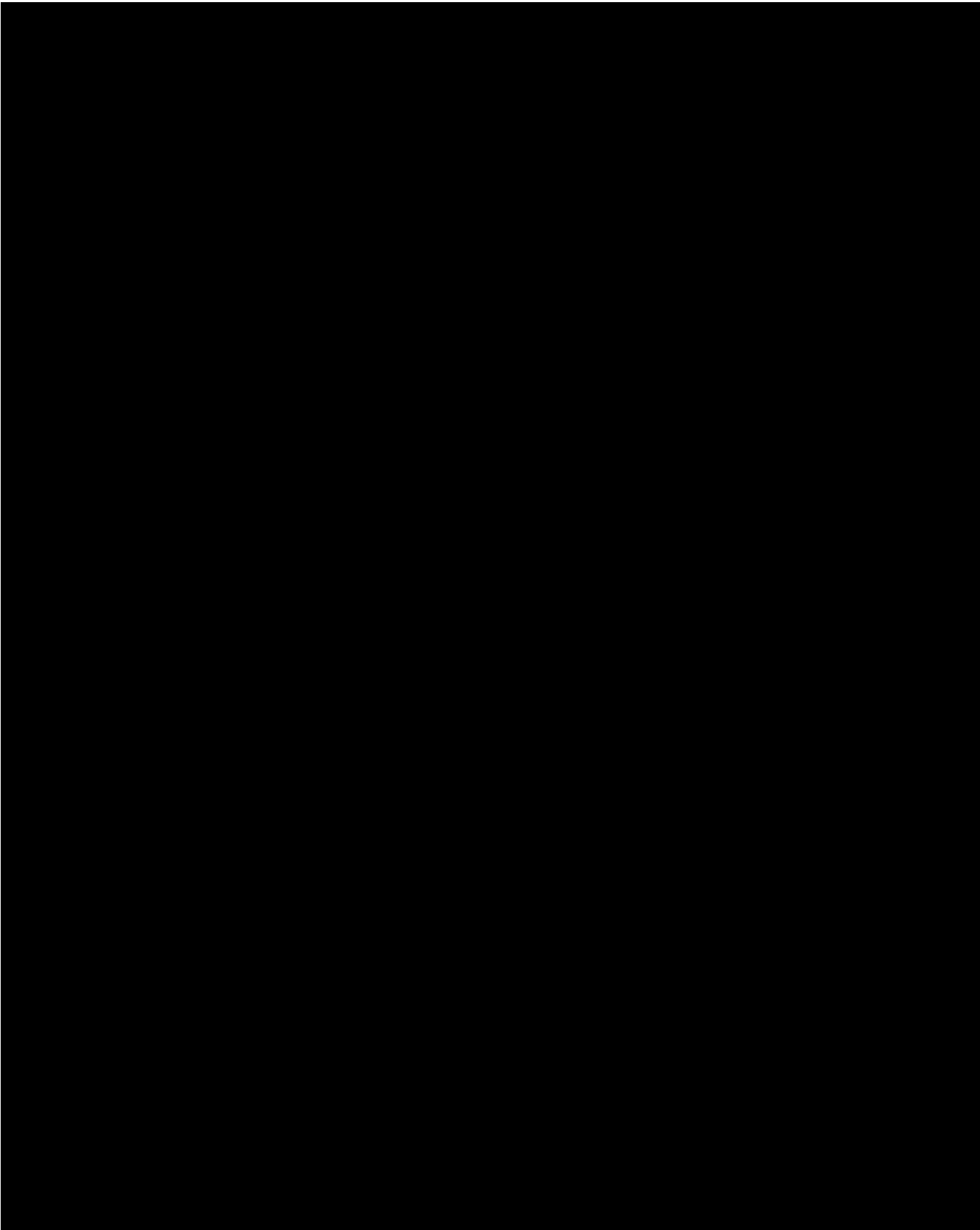


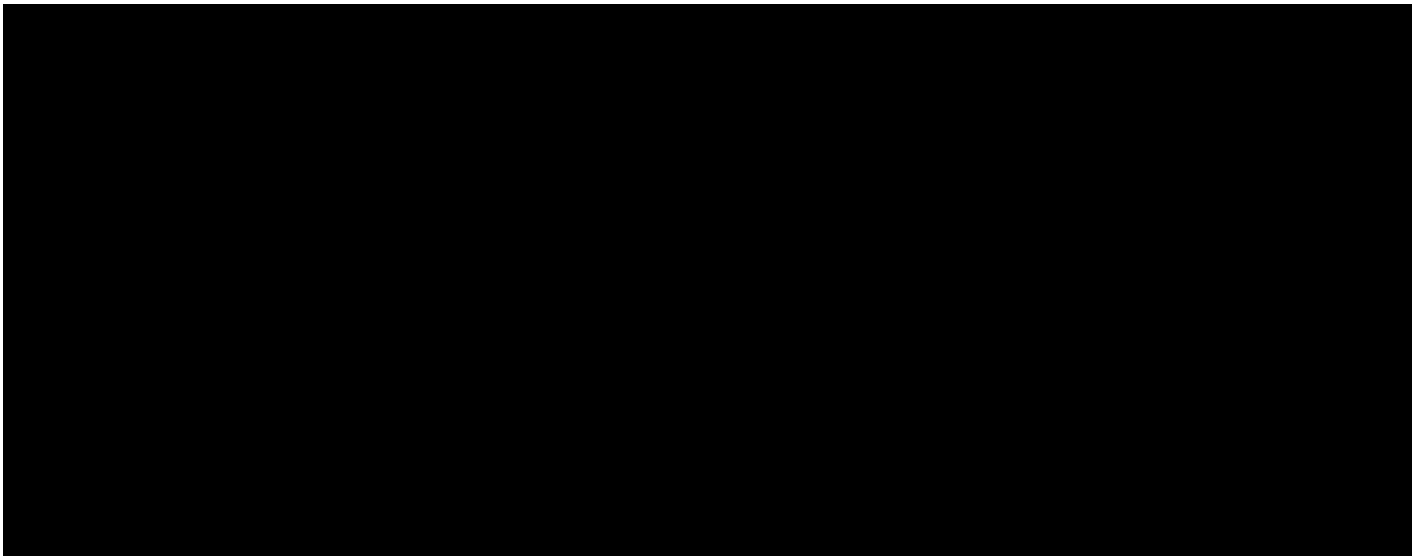












4.4.2 Open Interview Questions

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

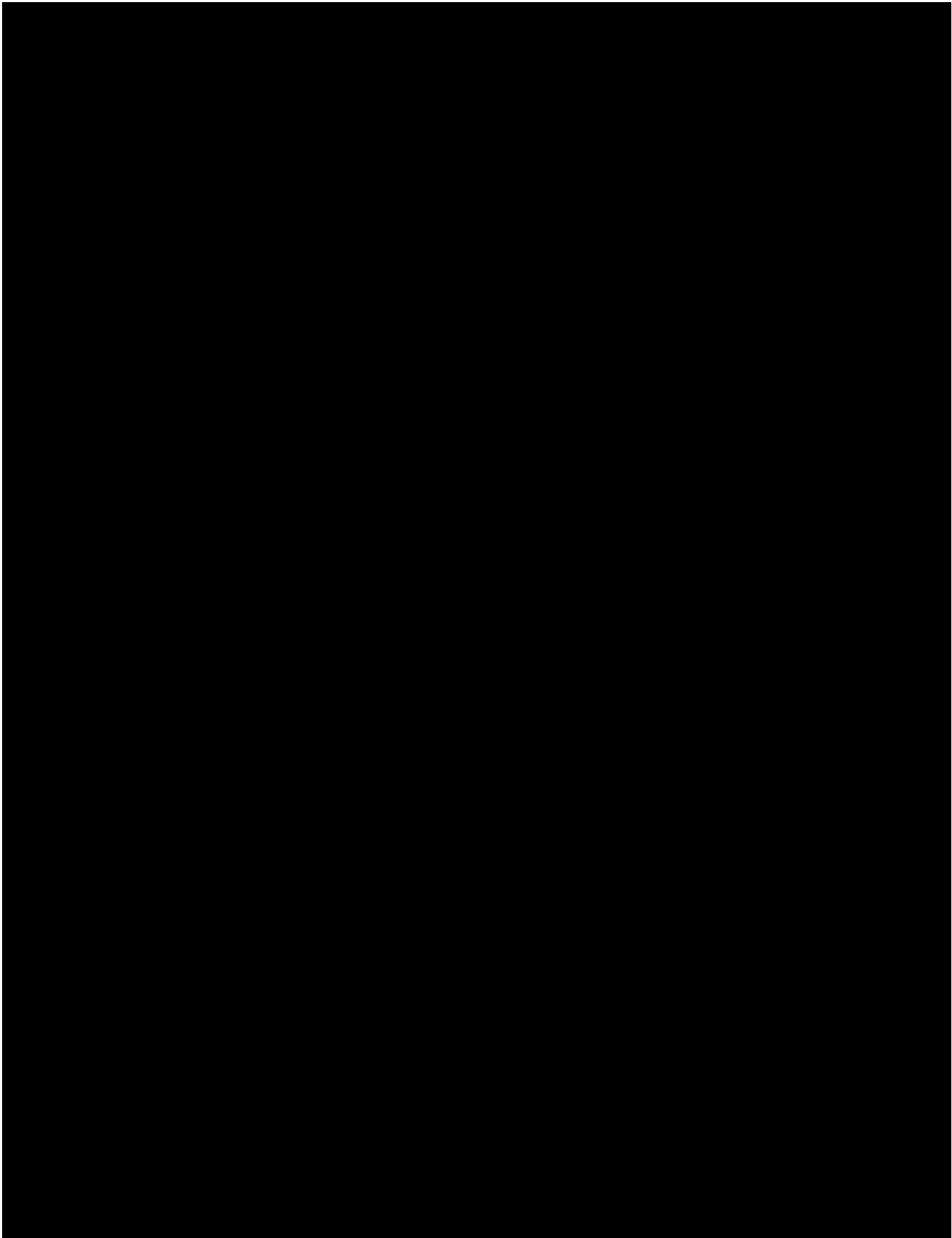
[REDACTED]

4.5 Outline of Scenarios for Pilot

[REDACTED]

[REDACTED]

[REDACTED]



4.5.2 “On border” crossing point check general scenario:

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	■	■	■	■	■	■	■	■

- [REDACTED]
- [REDACTED]

4.5.3 Description of specific situations:

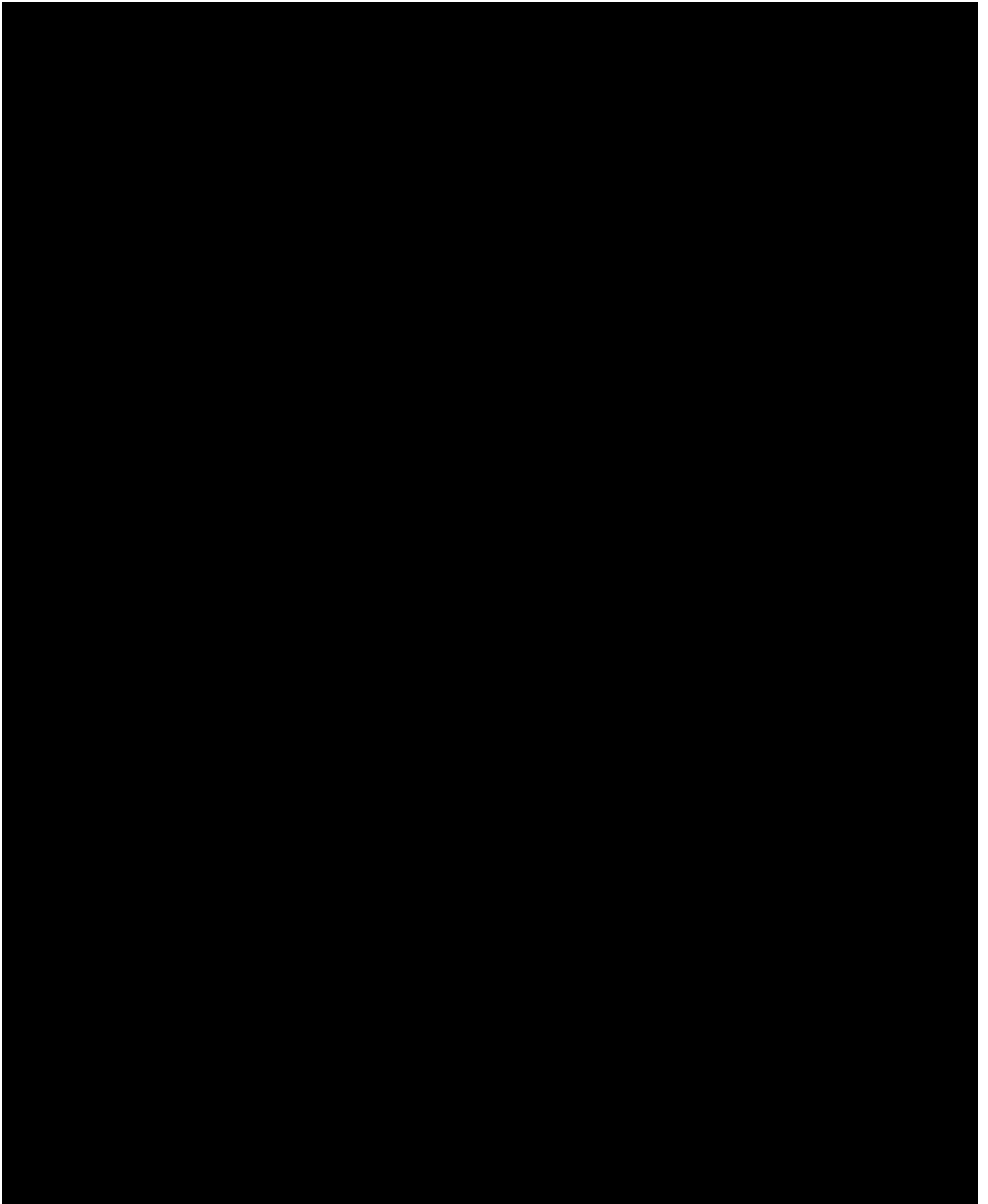
[REDACTED]

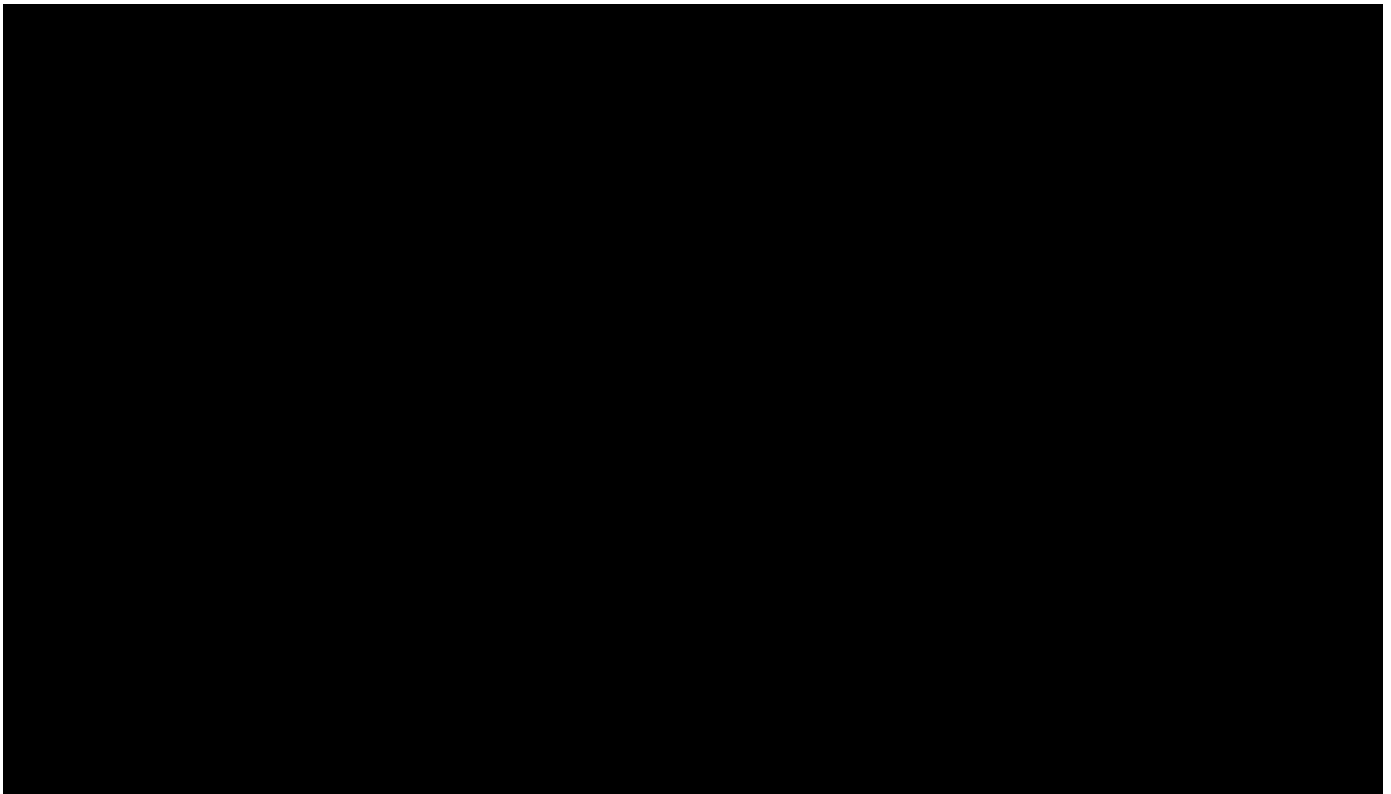
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

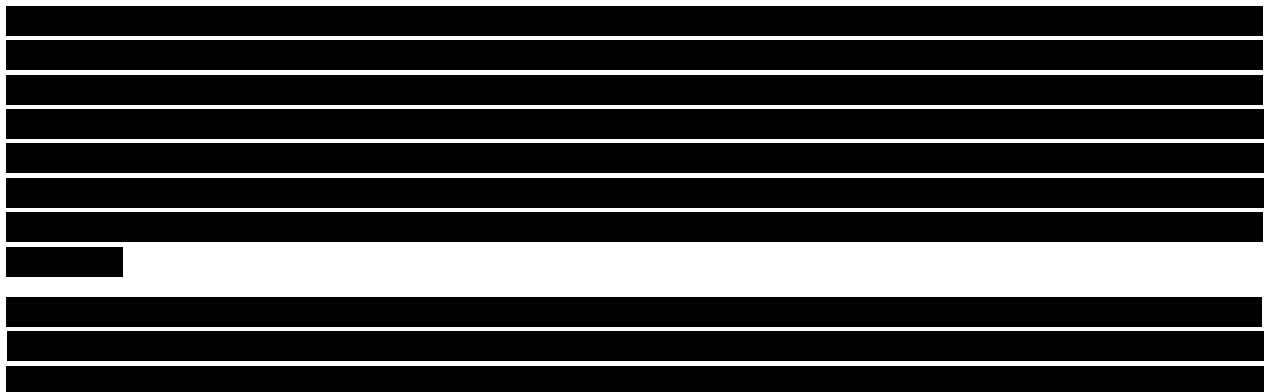


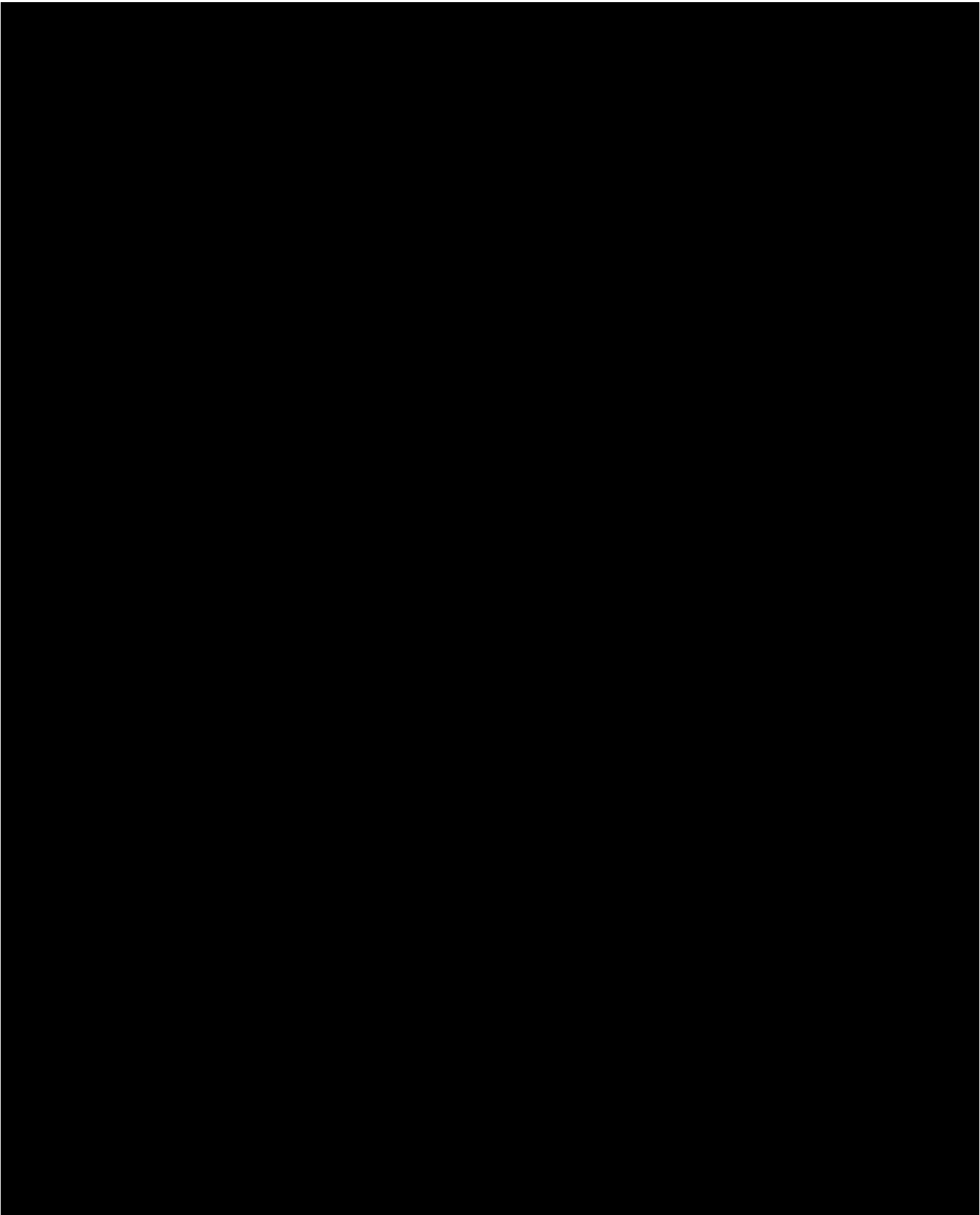


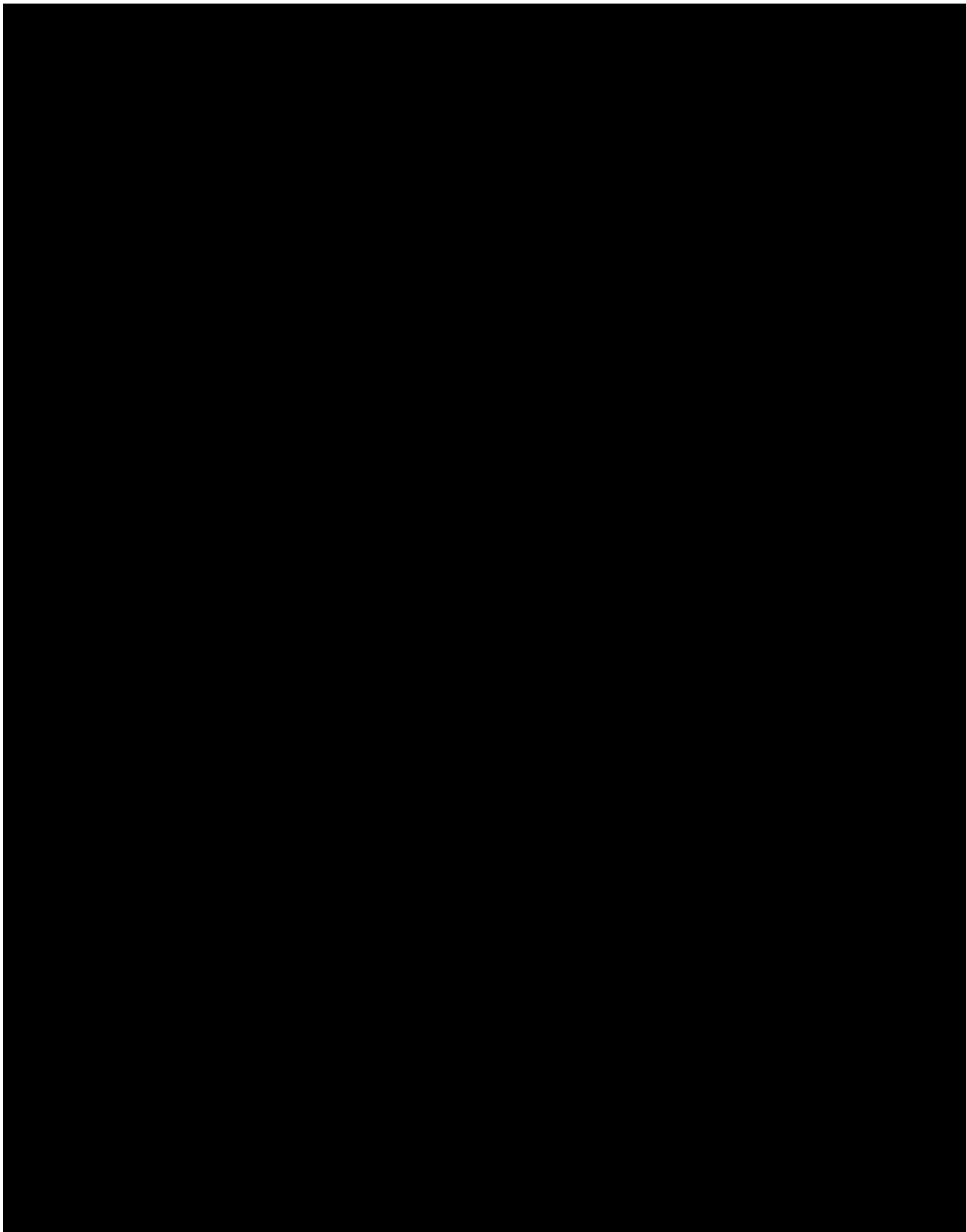
4.6 Current Situation at Candidate iCROSS pilot sites

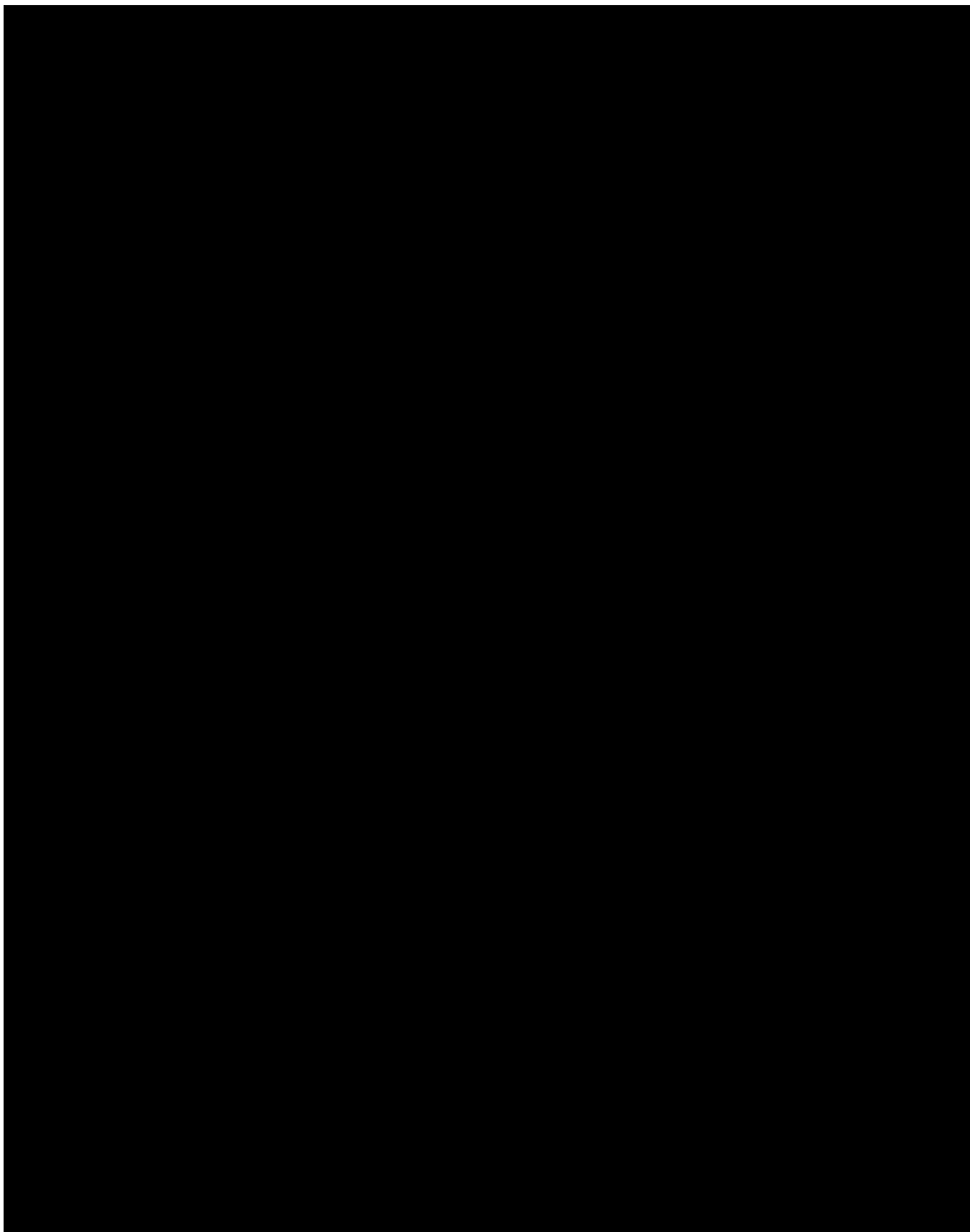


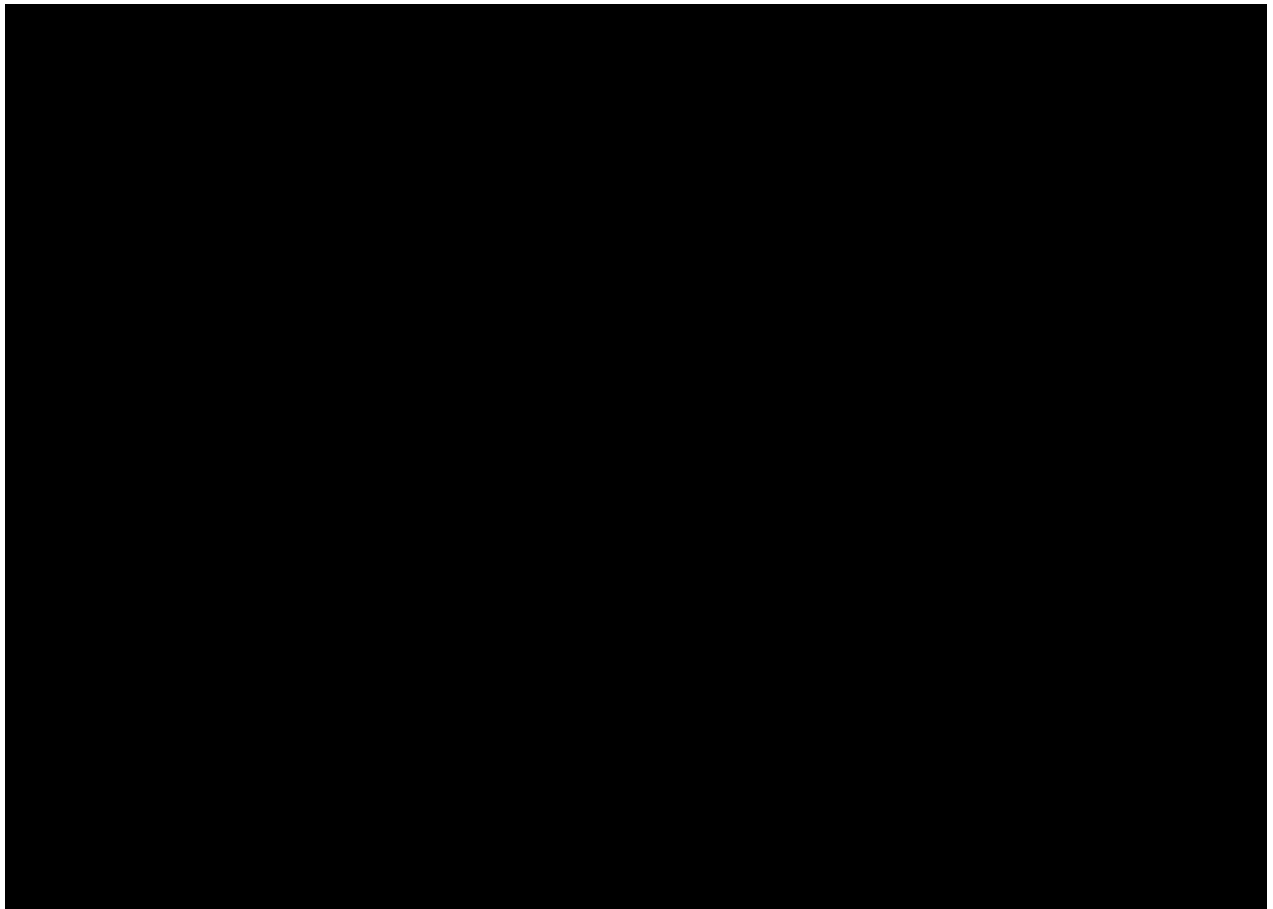
4.6.1 Tompa-Kelebia BCP









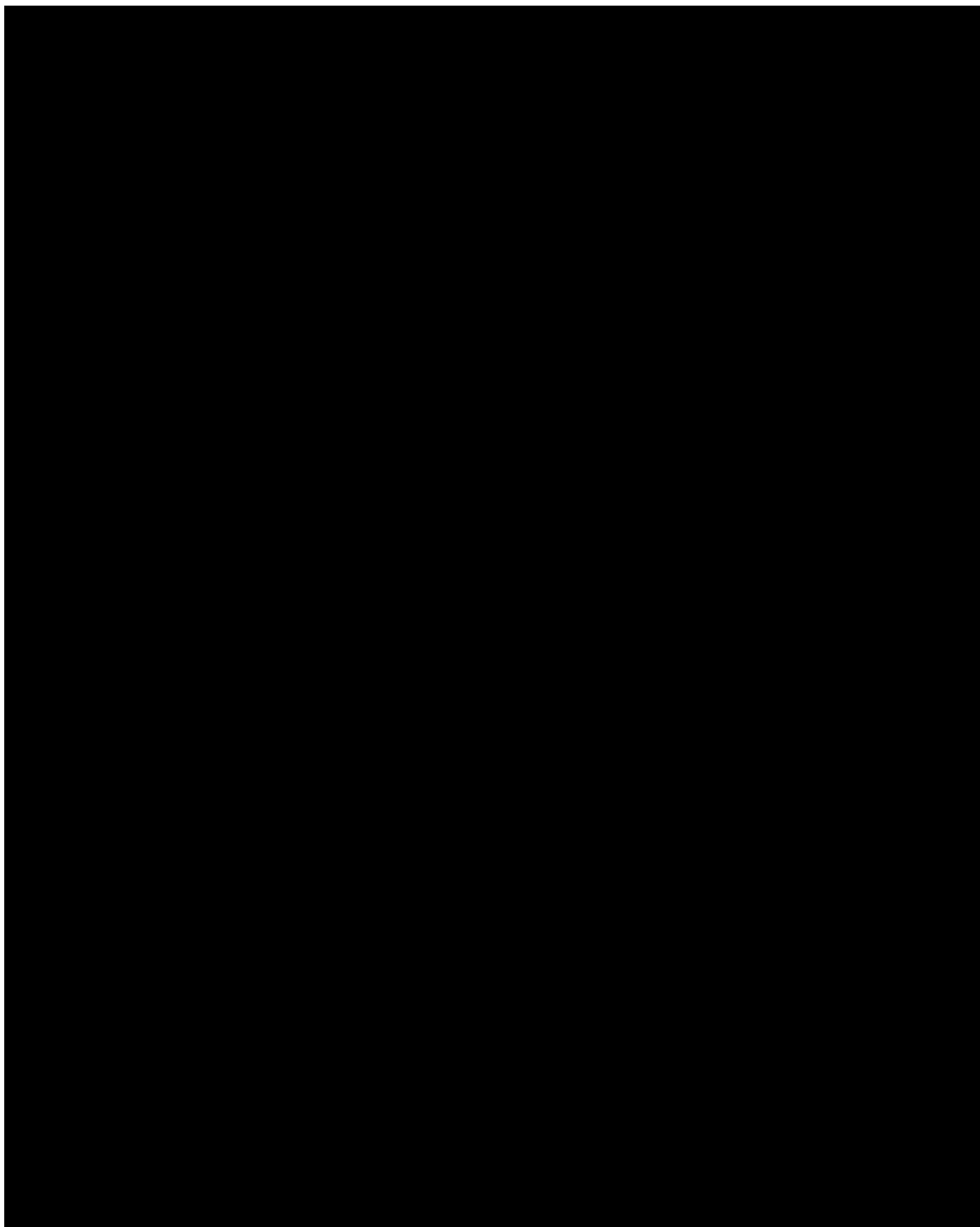


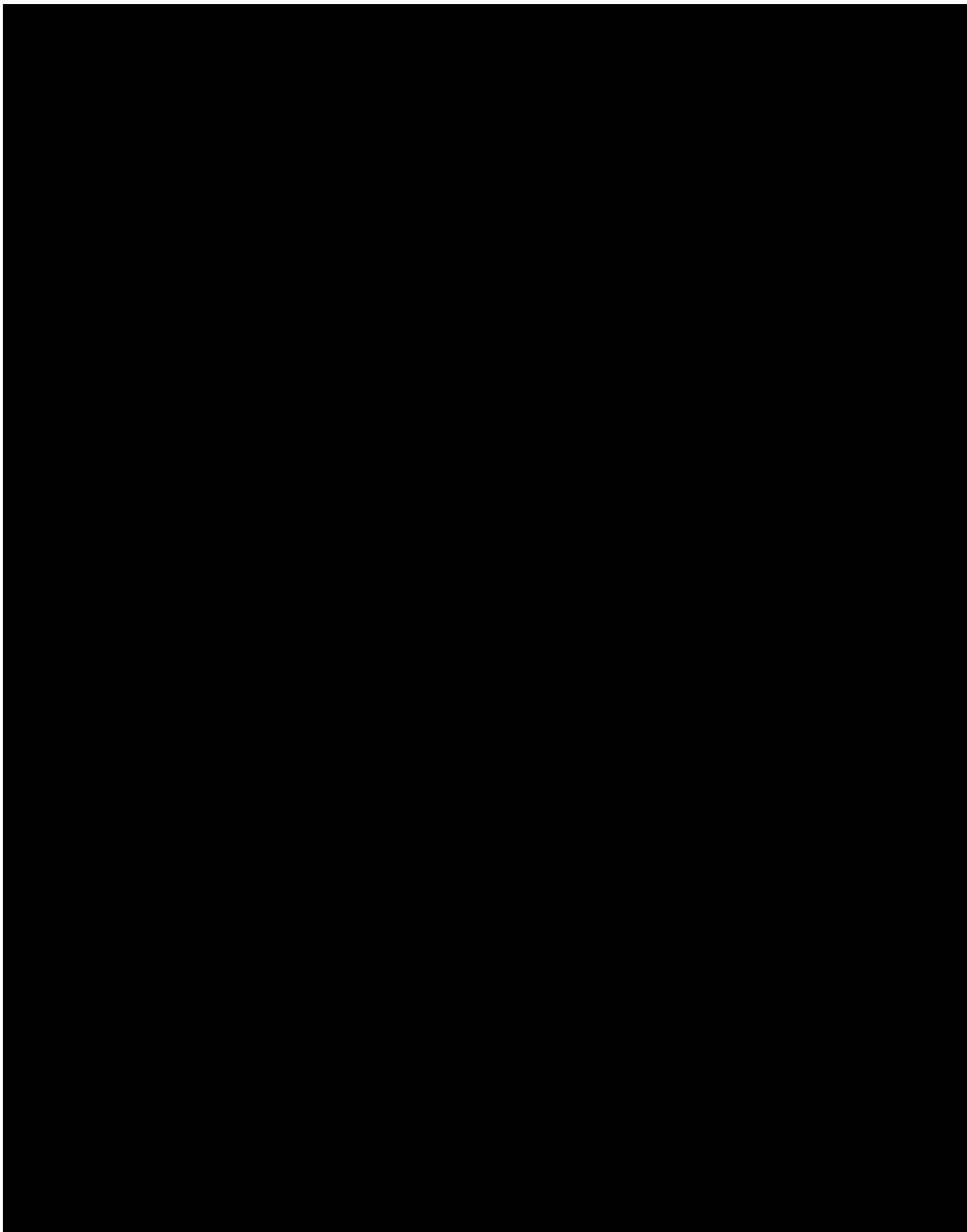
4.6.3 Terehova road BCP

[Redacted text block]

[Redacted text block]

[Redacted text block]





4.6.4 Zilupe railway BCP

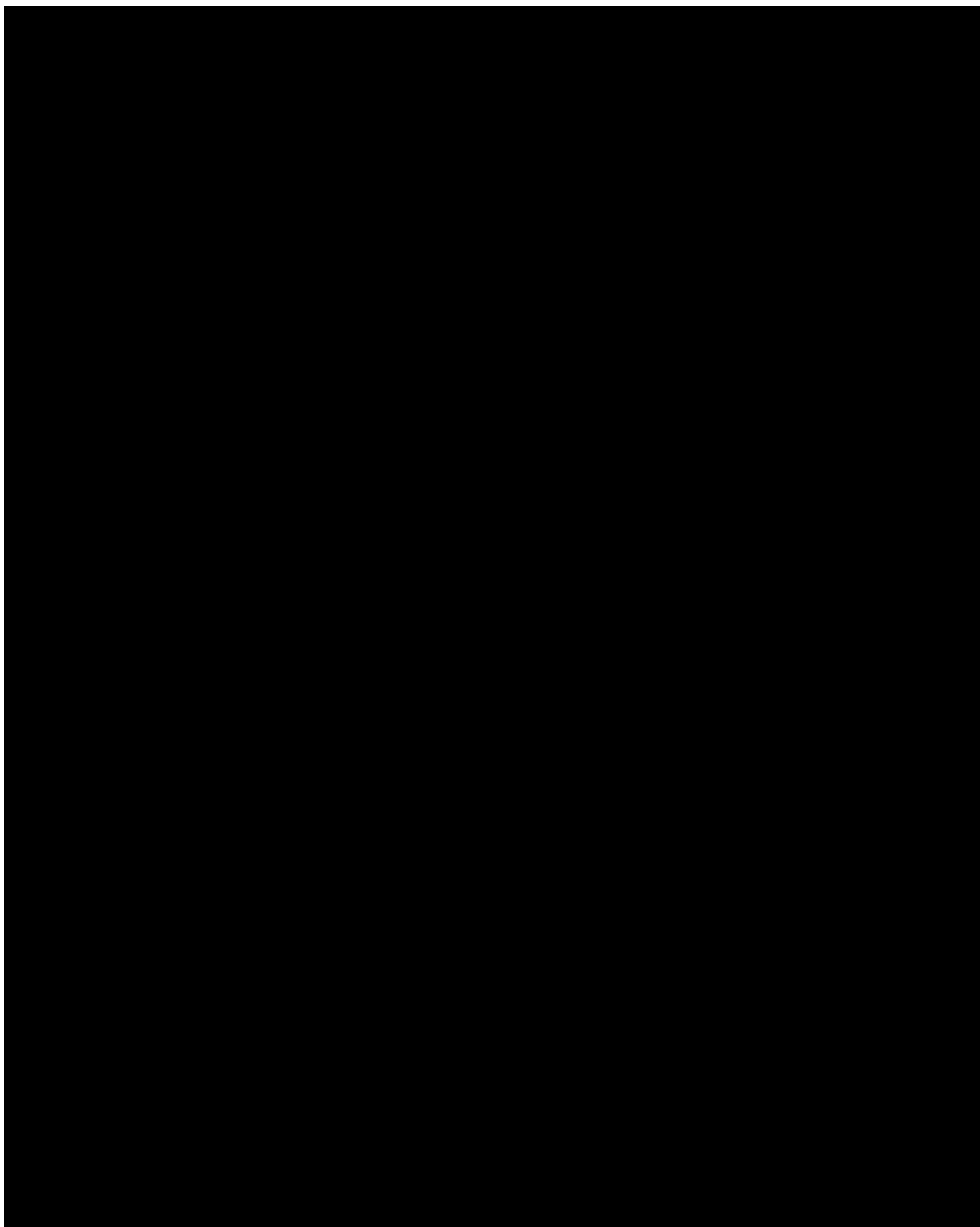
[REDACTED]

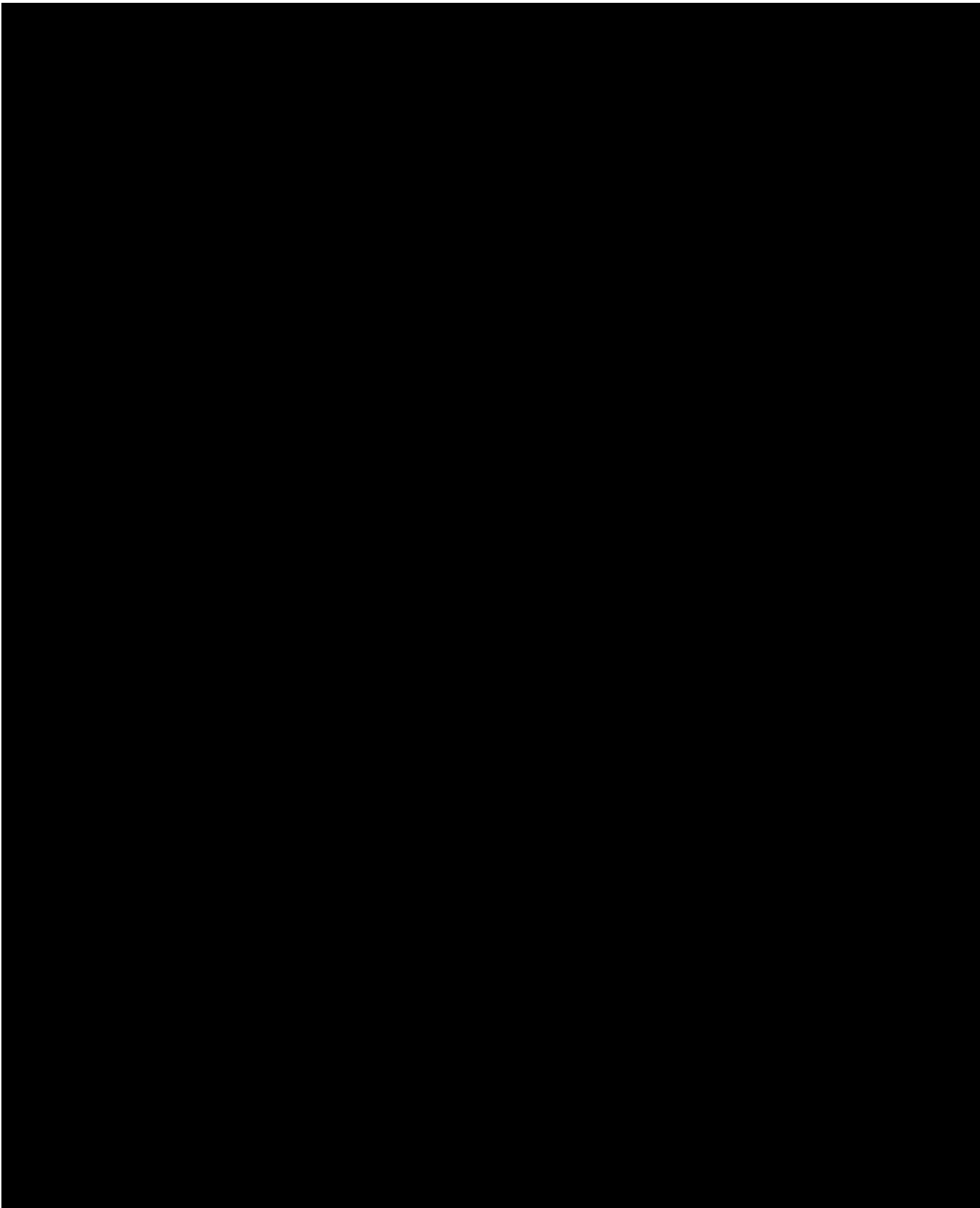
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

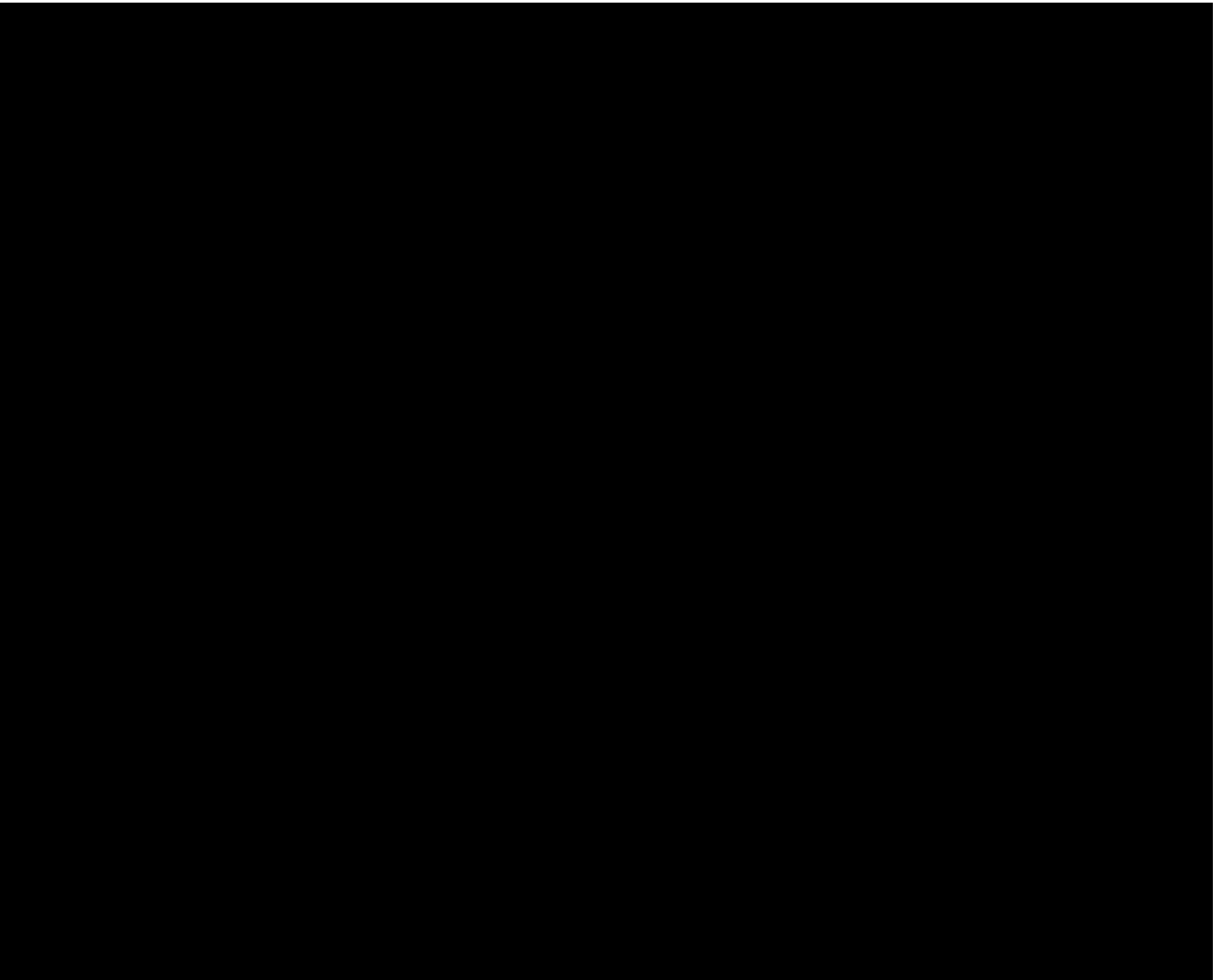
[REDACTED]

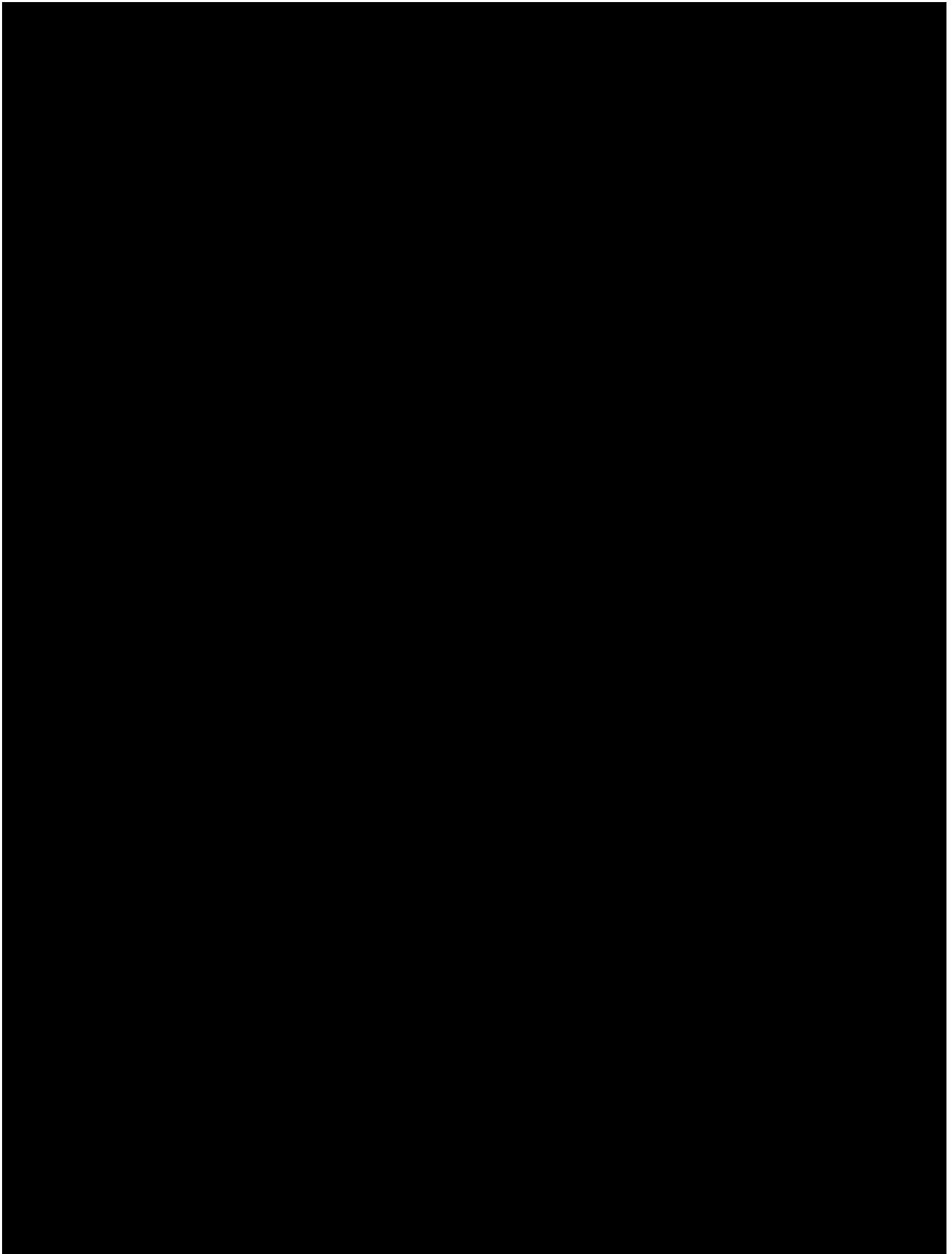


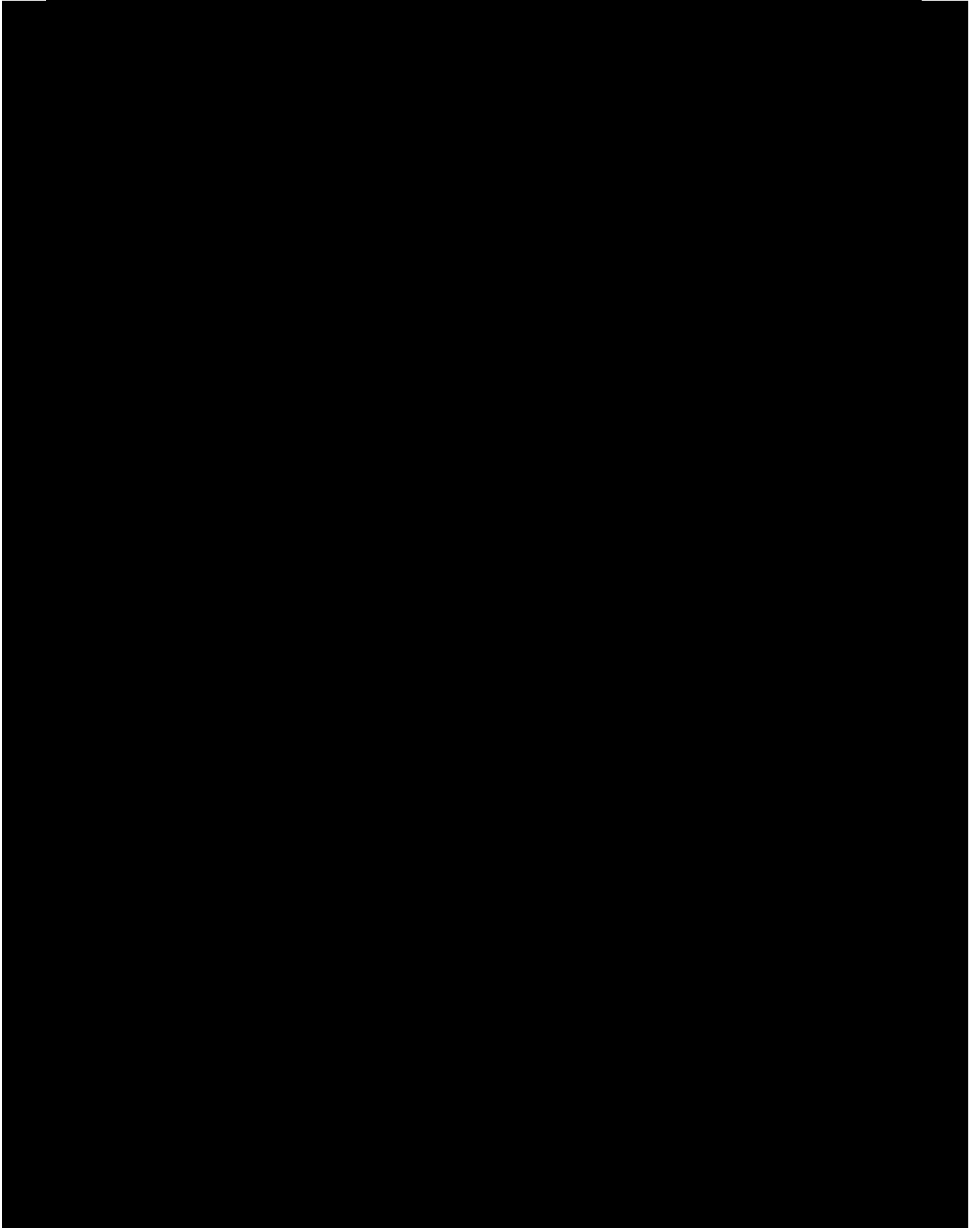


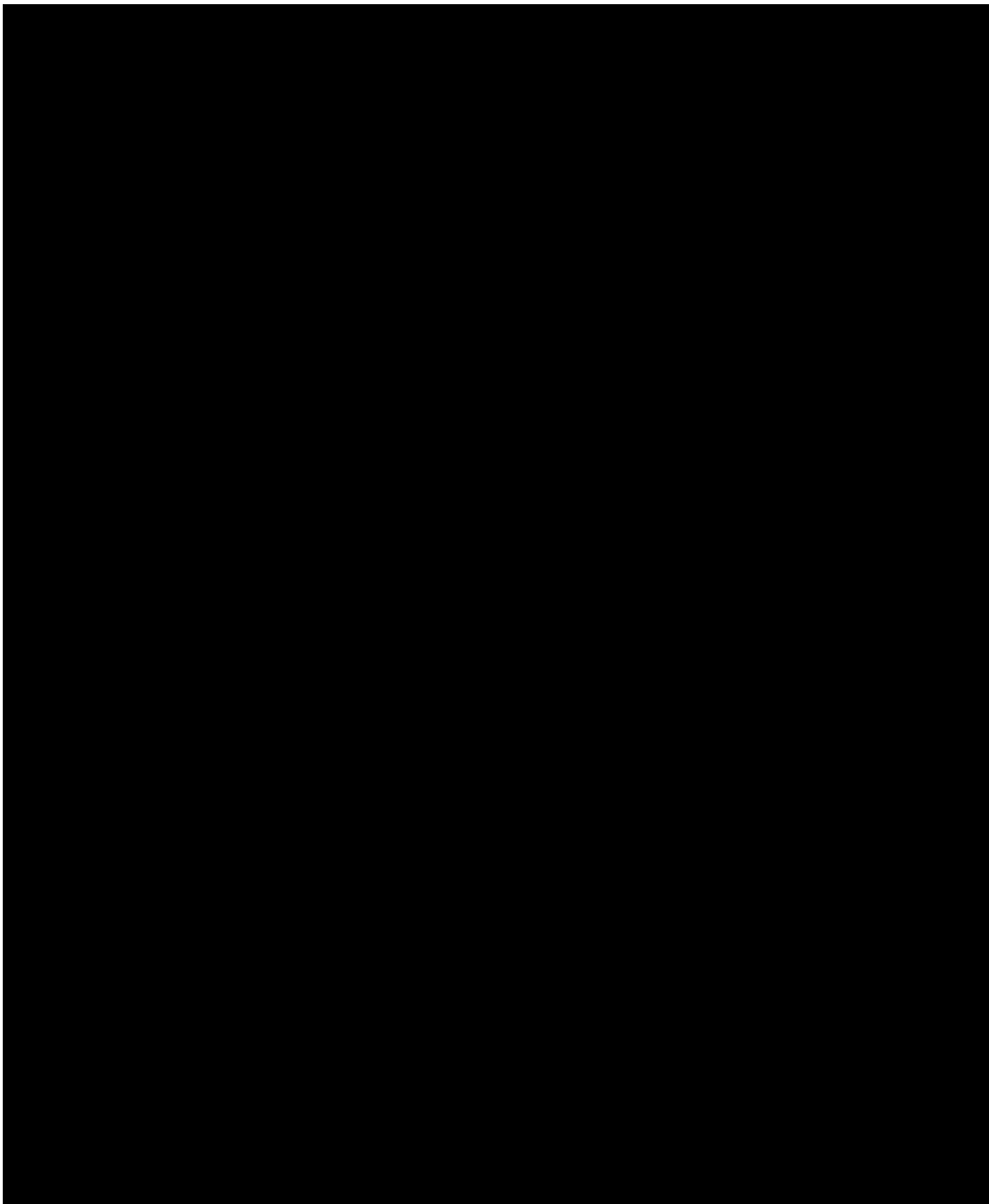


4.6.5 Eidomeni – Gevgeli BCP









4.6.6 Summary

[REDACTED]

5 User Requirements

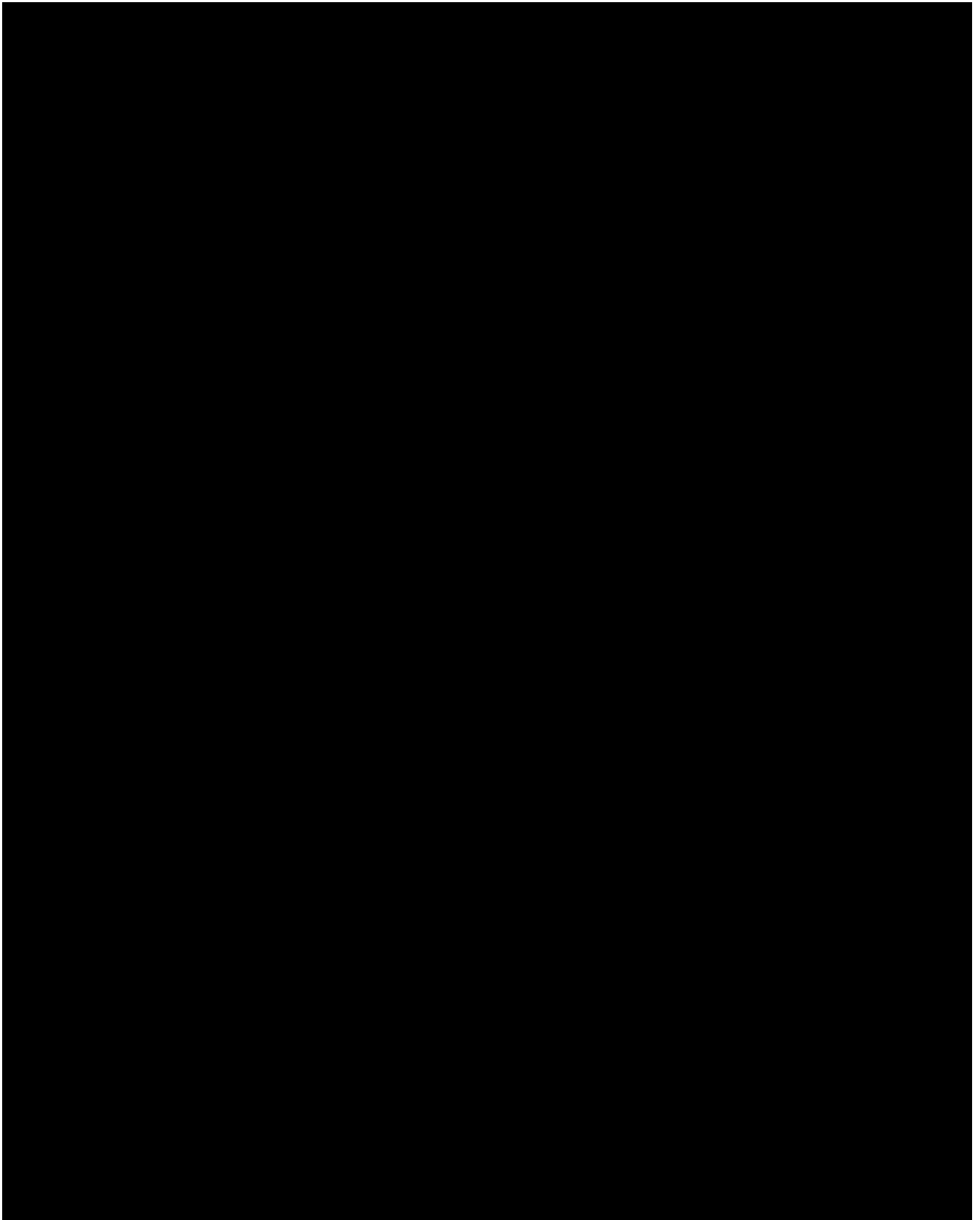
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

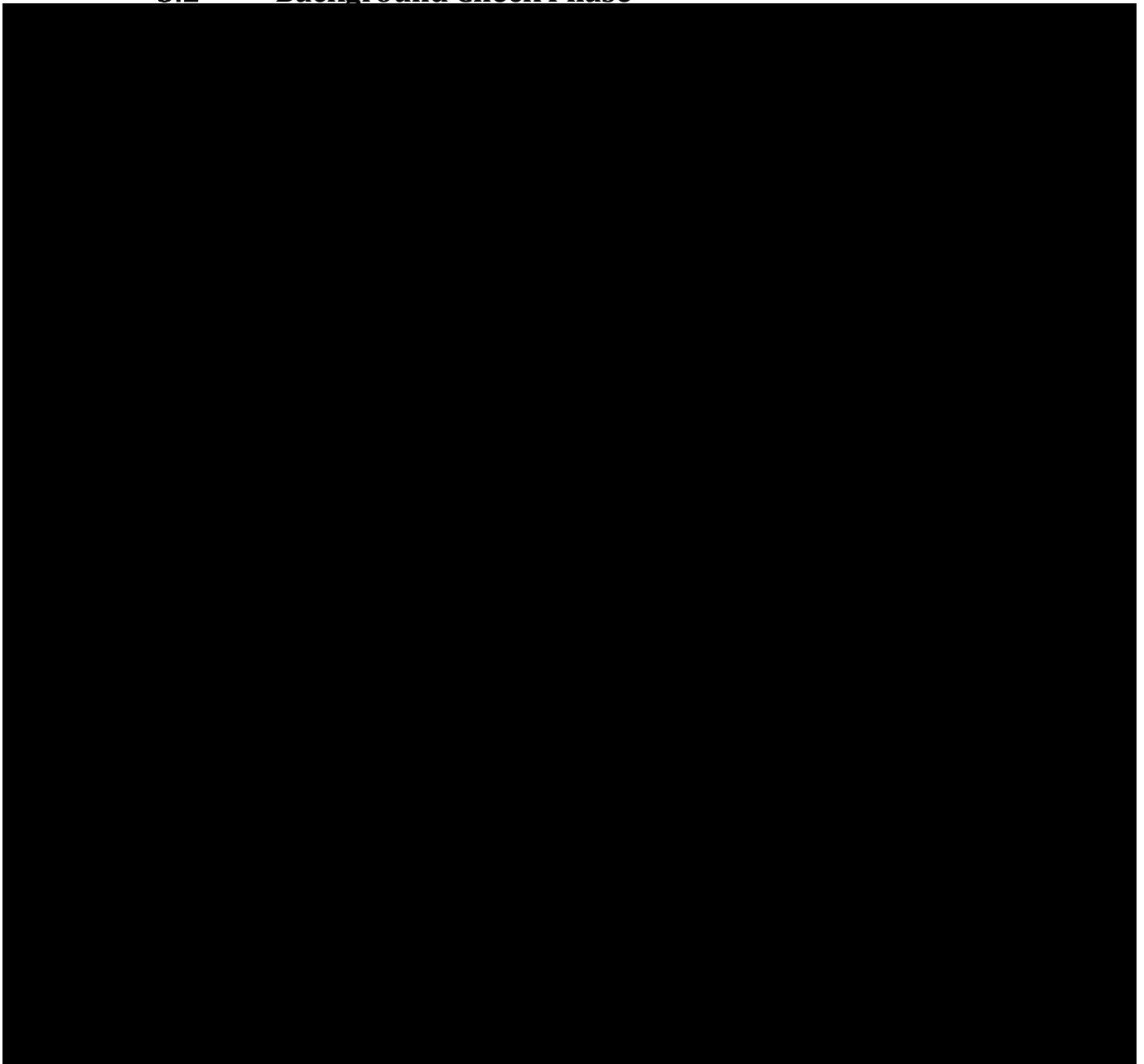
5.1 Pre-arrival Phase

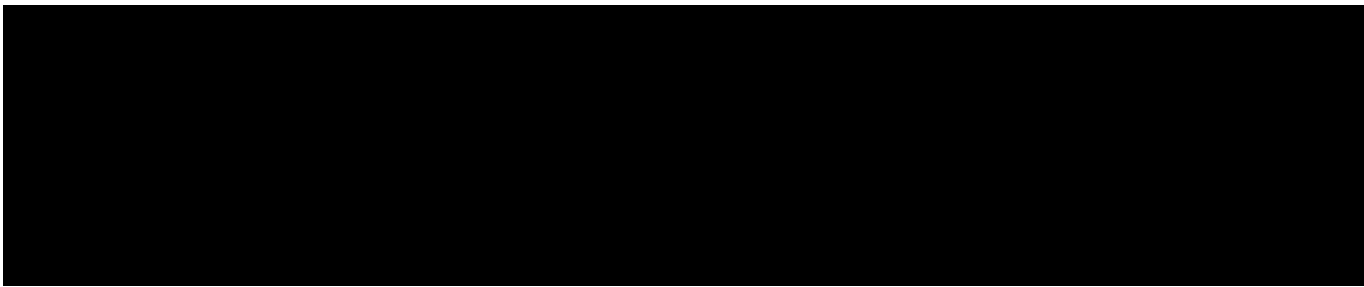
[REDACTED]



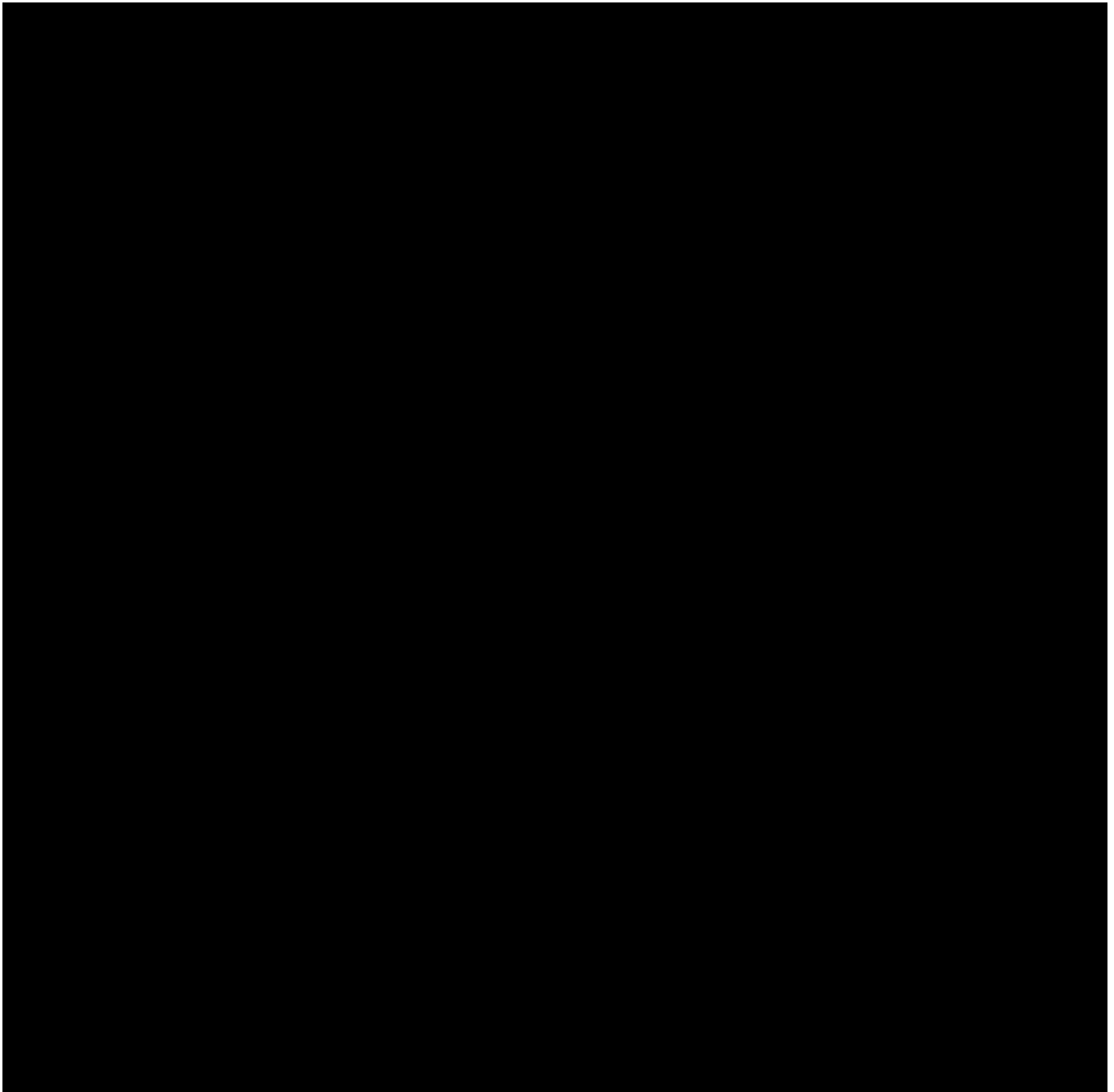


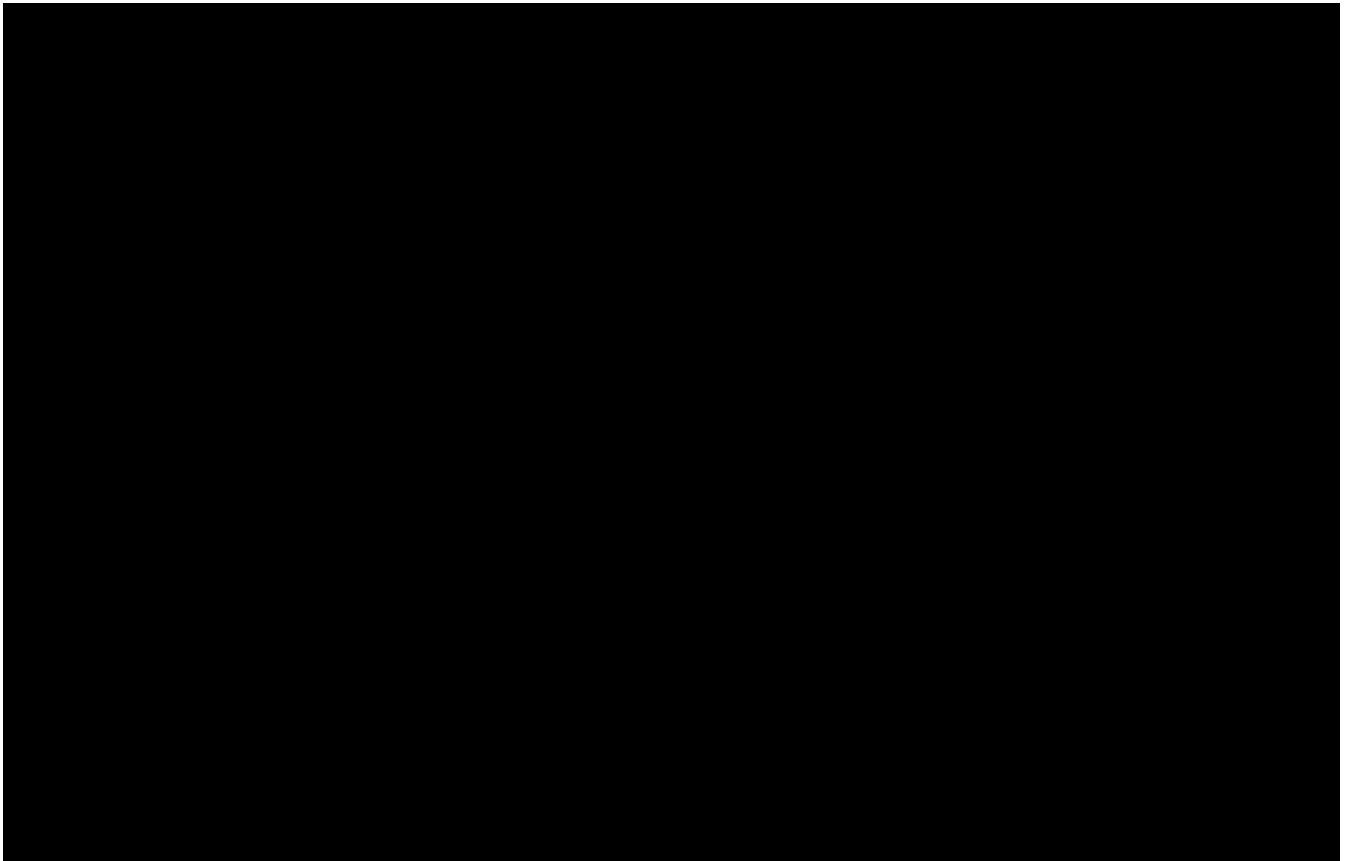
5.2 Background Check Phase



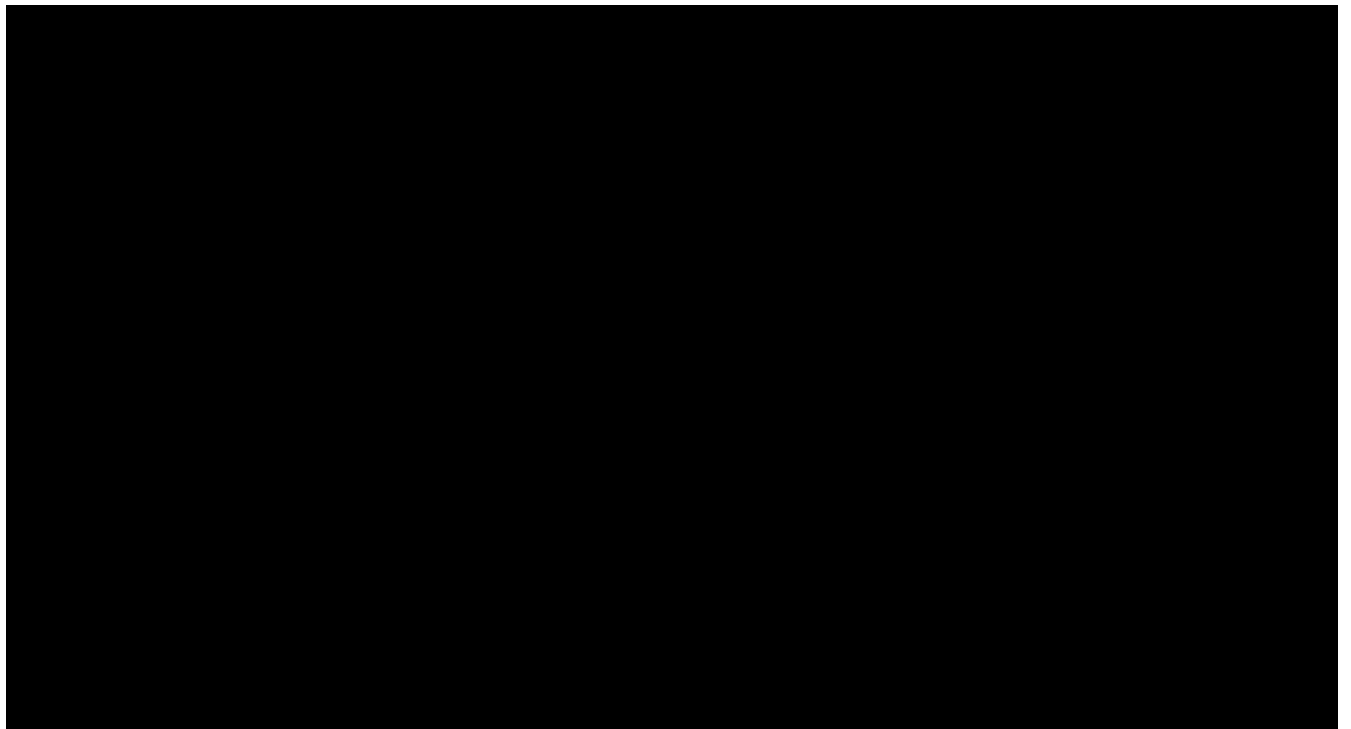


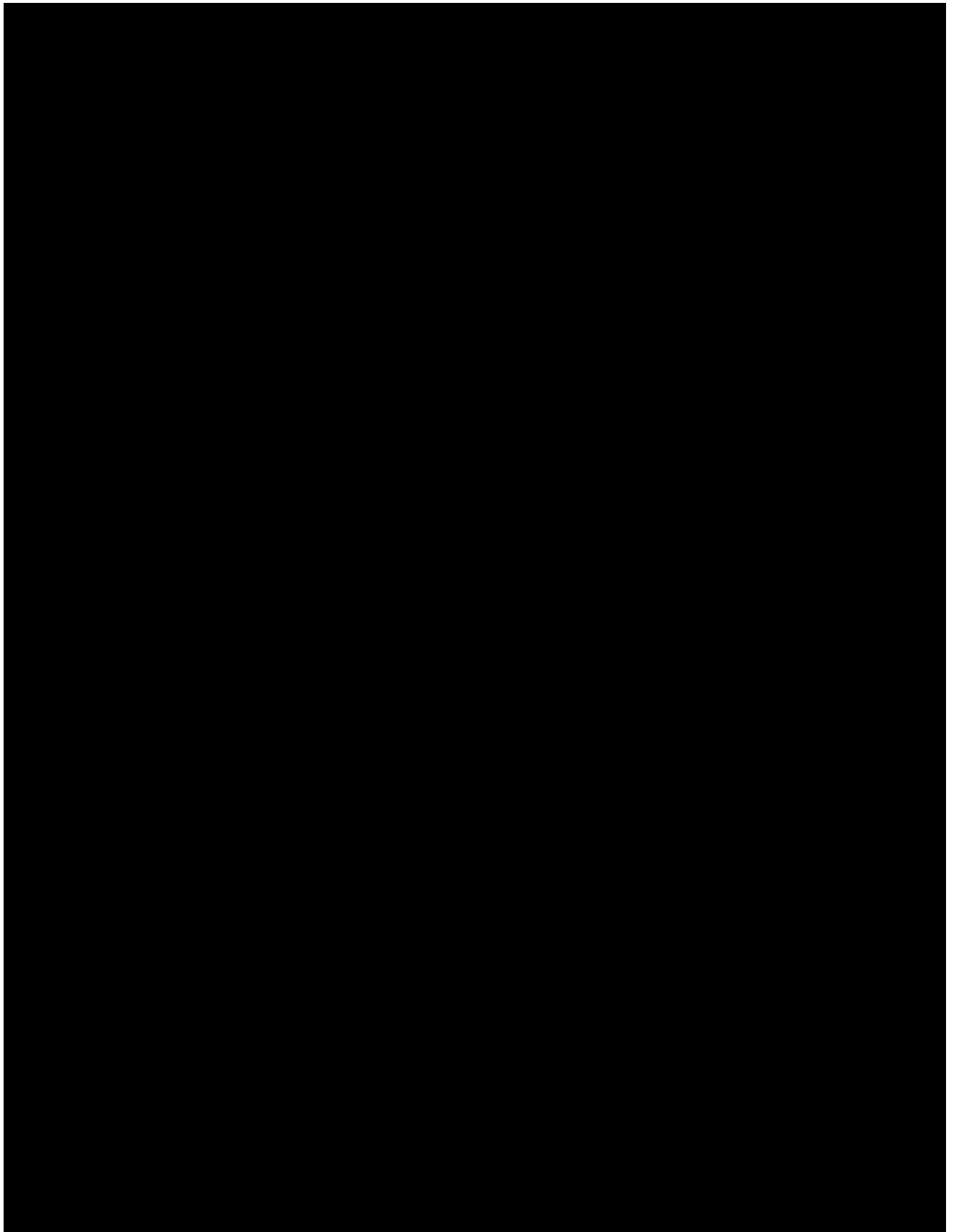
5.3 Border Check Phase

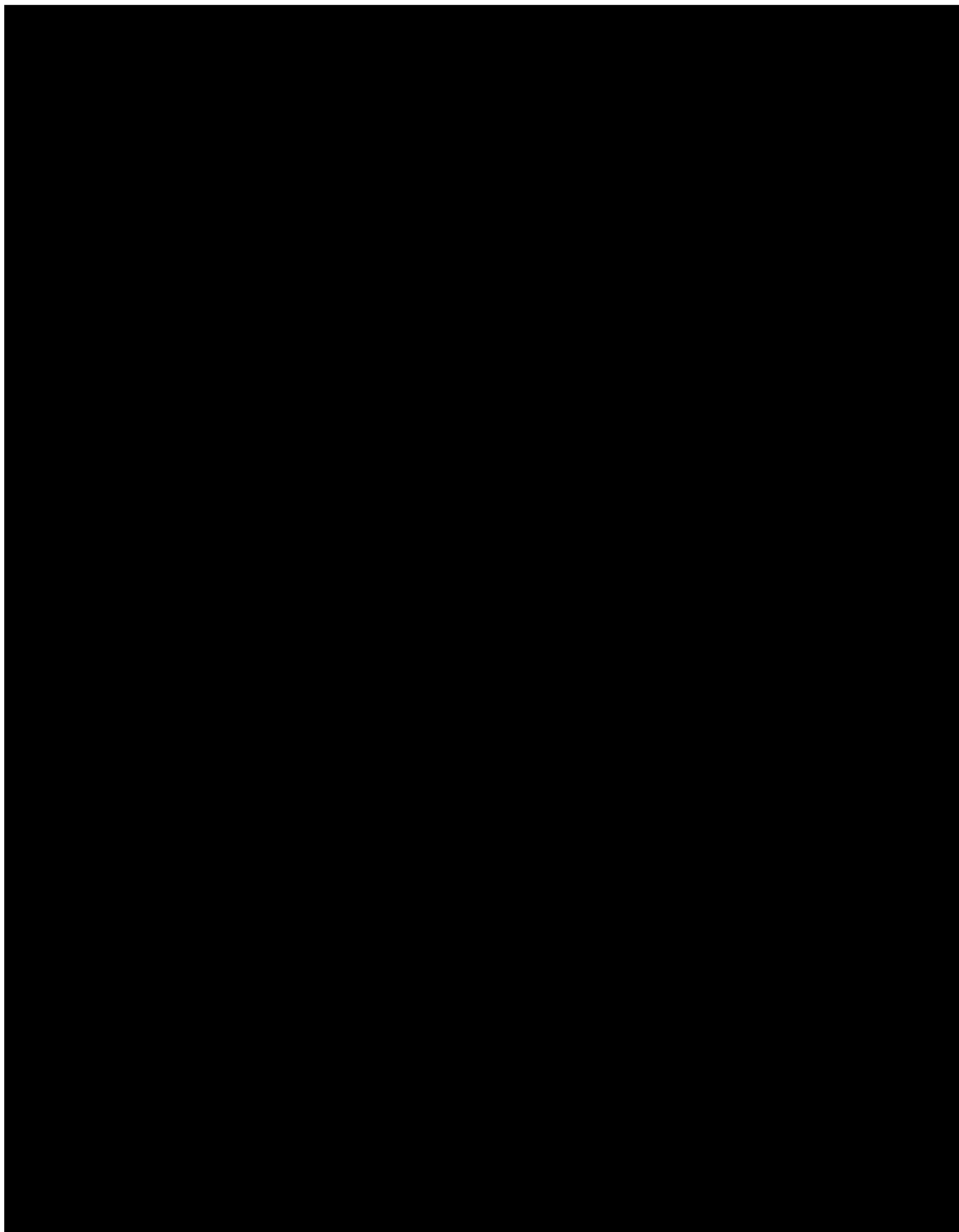


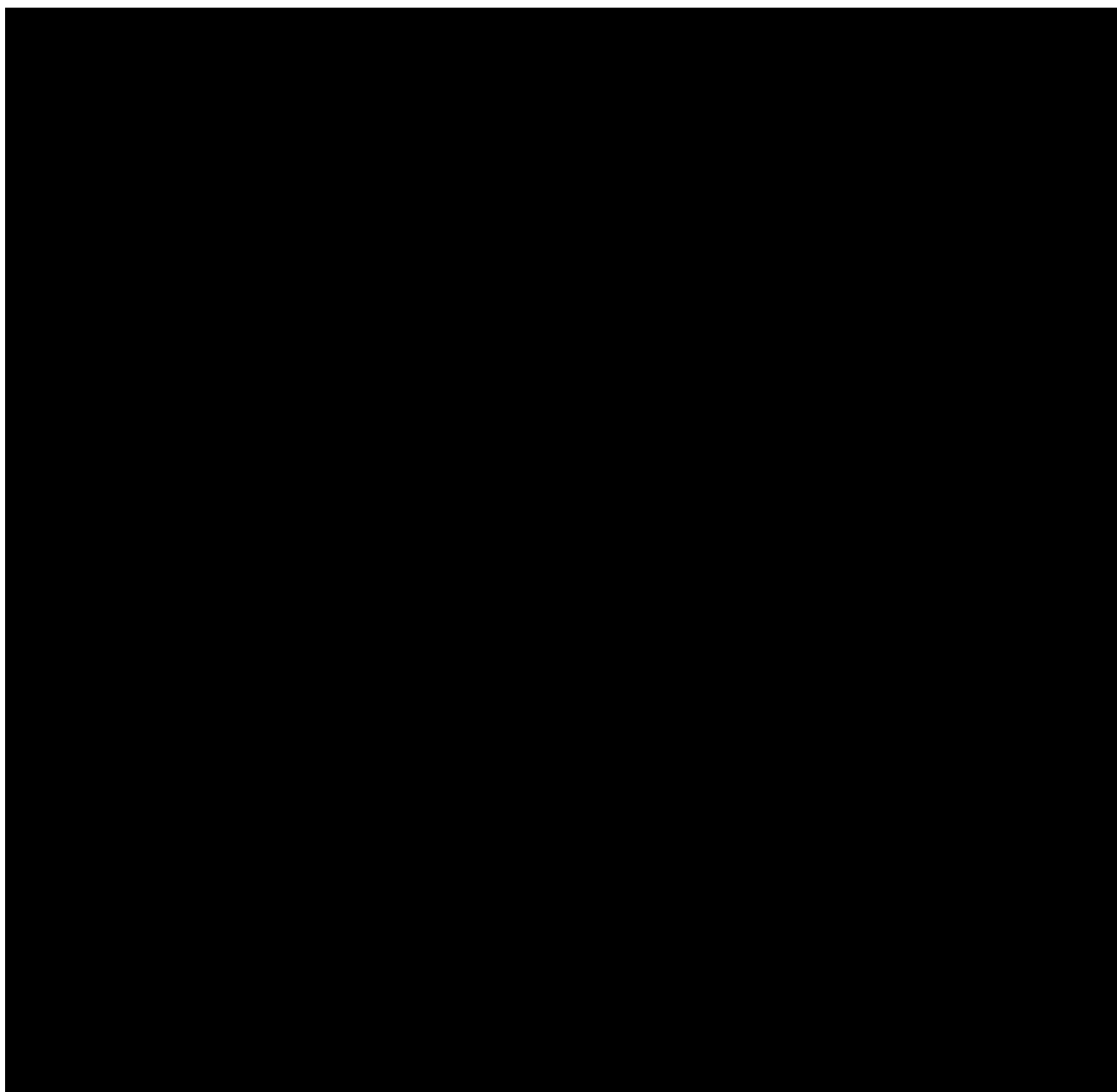


5.4 General Requirements









6 Conclusions

This document, D2.1, sets out to analyse the requirements of the iCROSS components, develop a comprehensive understanding of a range of issues required for the successful production of individual iCROSS deliverables and their coherent inter-working, and to support the meeting of those requirements under the EC grant contract. This document provides evidence that the consortium has achieved its four main objectives for requirements analysis: through its analysis of the concepts of border management, its review of the state of the art of technologies for border management, its capture of users' opinions and experience of border crossing and its systematic elicitation of general user requirements.

6.1 Accomplishments

Section 2 of this document provides a comprehensive review of the concepts of border management, first from a historical perspective then within the overarching context of EU border management. It then proceeds with practical analysis of the kinds of traffic, instrumentation solutions and border management workflows at road and rail border crossing sites of high importance to the EU (due to the volumes of traffic and natures of travellers). Reference sites are provided by our end users in Hungary, Latvia and Greece.

This is followed by a detailed and thorough review of the state of the art of border control technology (section 3). Again, there is an overview of the European context and of the particular technologies currently adopted by our end users. This leads to a review of cutting edge technologies, which could be used in iCROSS, including document authenticity analytics tools, automatic deception detection, biometrics, hidden human detection technologies and wireless communication networks.

The next section (4) develops the requirements capture methodology. This involves combining the user perspective (through Border Guard Officers / Manager interviews and surveys and a beyond-EU-wide travellers survey), an analysis of the state of the art captured in the previous section and the functional requirements emergent from the technological desiderata of the iCROSS system itself found in the DoW. The methodology is presented at a detailed level including specification, structuring and syntax of the requirements and the development of the questionnaires to capture the user perspective.

After analysis of the travellers' survey, Border Guard Officer surveys and Border Guard Officers / Manager interviews, this document outlines general scenarios for pilot testing, including the type of crossing being made, information to be checked and instrumentation used. These are then mapped on to the specific iCROSS components that will be called into play to make the checks for the particular scenario.

The requirements capture is concluded by enumerating the general user requirements in tabular form with a specific mapping onto the DoW.

6.2 Support for future work

The immediate benefit of D2.1 will be the support for the development of the detailed use cases, in functional and non-functional terms, in deliverable 2.2. These, in turn, will stimulate the relevant discussion on the reference architecture and the system's technical specifications.

iCROSS proceeds from WP2 to WP3 (Technological Components and Subsystems Development) and WP4 (Development of the iCROSS Software Platform and related interfaces). Internally, sections 2 and 4 of this document (D2.1) provide background contextual information which informs sections 3 (State of The Art Technology Review) and 5 (User Requirements). Therefore, this document shall indicate where the work should begin at the beginning of the Work Packages 3 and 4, but also it shows the development paths, by defining the parameters of the practical and possible in response to user needs.

6.3 Contribution to Roadmap

In terms of the iCROSS Roadmap, this document's most salient contribution is to the achievement of milestones 1 (Reference architecture and component specifications), 2 (First version of all tools) and 3 (Early version of the integrated prototype – limited functionalities) by providing the necessary know-how which will be consumed by the design processes. It also makes a secondary contribution to milestone 4 (Final version of the integrated prototype and portable unit) as milestones 2 and 3 are necessary precursors for 4. Through its development of use-cases and scenarios it also makes a direct contribution to the design of our evaluation methodology for milestone 5 (Evaluation report of final prototype pilot deployment). See page 120 of the Grant Agreement for details of the project milestones.

In terms of deliverables, this document contributes to:

- D2.2 Reference Architecture and components
- D3.1 Data Collection Devices-specifications
- D3.2 First version of all technological tools
- D4.1 First version of the iCROSS software platform
- D5.2 Early version of the integrated prototype (limited functionality)
- D5.3 Early version of the portable unit for border guards
- D7.6 Yearly communication report

6.4 Summary

Therefore, the overall conclusion is that iCROSS deliverable 2.1 has made a useful and significant contribution to over-arching workpackages and concrete deliverables, and consequently to the future success of the iCROSS project.

7 References

- 3GPP (2009), Technical Specification Group Services and System Aspects Service aspects; Services and Service Capabilities", TS 22.105 V6.0.0 (2002-09) (Release 6), [online] Available at: <http://www.3gpp.org> [Accessed 23 Oct. 2016].
- Abc4eu.com, (2016). Abc4eu-project Official Website. [online] Available at: abc4eu.com [Accessed 11 Oct. 2016].
- Access-is.com, (2016). Access-is Official Website. [online] Available at: <http://www.access-is.com/ocr640-desktop-full-page-passport-id-reader.php> [Accessed 07 Oct. 2016].
- ACXIS project (2013). Project ID: 312998, Funded under: FP7-SECURITY, SEC-2012.3.4-1 - Research on "automated" comparison of x-ray images for cargo scanning with reference material (use of historic images in an automated environment) to identify irregularities - Capability Project, EU.
- CORDIS Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/110003_en.html
- Aggelopoulos, E. G., Karabetsos, E., Constantinou, F. and Uzunoglu, N.K., (1996). Mobile microwave sensor for detection of trapped human beings. Measurement: Journal of the International Measurement Confederation. 18(3), 177-183.
- Anil K. Jain, Patrick Flynn, Arun A. Ross. (2008) Handbook of Biometrics. ISBN 978-0-387-71041-9
- Arh.hu, (2016). Arh Official Website. [online] Available at: <http://arh.hu/index.php/en/products/passport-id-readers/prmc.html> [Accessed 07 Oct. 2016].
- Arthur, C. 2009. Government data shows £2.4m 'lie detection' didn't work in 4 of 7 trials. [online] Available at: <https://www.theguardian.com/news/datablog/2009/mar/19/dwp-voice-risk-analysis-statistics>. [Accessed 30 Nov. r 2016].
- Bartlett, M.S., Littlewort-Ford, G., Movellan, J., Fasel, I. and Frank, M., The Regents Of The University Of California and The Research Foundation Of State University Of New York, 2014. *Automated facial action coding system*. U.S. Patent 8,798,374.
- Bartlett, M.S., Hager, J.C., Ekman, P. and Sejnowski, T.J., (1999). Measuring facial expressions by computer image analysis. *Psychophysiology*, 36(02), 253-263.
- BenFred, S. Bonald, T. Proutiere, A. Régnié, G. Roberts, J.W. (2001) Statistical bandwidth sharing: a study of congestion at flow level. In Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '01). ACM, New York, NY, USA, 111-122. DOI=<http://dx.doi.org/10.1145/383059.383068>.
- Bianchi, G. (2000). Performance analysis of the IEEE 802.11 distributed coordination function, in *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535-547, doi: 10.1109/49.840210
- Bimpas, M., Paraskevopoulos, N., Nikellis, K., Economou, D. and Uzunoglu, N. (2004). Development of a Three Band Radar System for detecting Trapped alive humans under building ruins. *Journal PIER*. 49, 161-188.

- Blazacq, T., & Carrera, S. (2005). *Migration, Borders and Asylum: Trends and Vulnerabilities in EU Policy*. Brussels: Centre for European Policy Studies.
- Blenkinsopp, J. (1987). The mission of Udjahorresnet and those of Ezra and Nehemiah. *Journal of Biblical Literature*, 106(3), 409-421.
- Bogaard, G., Meijer, E.H., Vrij, A. and Merckelbach, H., (2016). Strong, but wrong: lay people's and police officers' beliefs about verbal and nonverbal cues to deception. *PloS one*, 11(6), p.e0156615.
- Bodega-project.eu, (2016). Bodega-project Official Website. [online] Available at: <http://bodega-project.eu/> [Accessed 11 Oct. 2016].
- Bonassies, P. (1969) *La loi du pavillon et les conflits de droit maritime*.
- Bonald, T. (2007). Insensitive traffic models for communication networks, *Discrete Event Dynamic Systems*, vol. 17, 405–421.
- Boehm, F. (2011). *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. Heidelberg: Springer Science & Business Media.
- Bonassies, P. (1969). *La loi du pavillon et les conflits de droit maritime*. In H. A. Law (Ed.), *Collected Courses of the Hague Academy of International Law*, Nijhoff: Brill, Vol. 129, 505-629.
- Bossong, R., & Carrapico, H. (2016). *Eu Borders and Shifting Internal Security: Technology, Externalization and Accountability*. Heidelberg: Springer.
- Brincker, R., Lago, T., Andersen, P., and Ventura, C. (2005). Improving the classical geophone sensor element by digital correction. *Tech. rep., Pinocchio Data Systems, Feb. 2005*.
- Brouwer, E. (2008). *Digital Borders and Real Rights: Effective Remedies for Third-Country National*. Leiden: Martinus Nijhoff Publishers.
- Burquist, J. and Boockholdt, D. (2001). System and method for automatic document verification. US 20020145747 A1.
- Caso, L., Gnisci, A., Vrij, A. and Mann, S., (2005). Processes underlying deception: an empirical analysis of truth and lies when manipulating the stakes. *Journal of Investigative Psychology and Offender Profiling*, 2(3), 195-202.
- Cbord-h2020.eu, (2016). Cbord-project Official Website. [online] Available at: <http://www.cbord-h2020.eu/> [Accessed 11 Oct. 2016].
- Changzhi, L., Cummings, J., Lam, J., Graves, E. and Wu, W. (2009). Radar Remote Monitoring of Vital Signs. *IEEE Microwave Magazine*. February 2009, 47-56.
- Chao, C. (2012). *Automatic Ultra-Wide-band Radar System for Life Detection of Hidden Humans. Dissertation, Christian-Albrechts-Universität zu Kiel*.
- Chen, K. M., Misra, D., Wang, H., Chueng, H.L. et al., (1986). An X-band M/W life-detection system. *IEEE Trans. Biomedical Eng.* BME-33, 697–701.
- Chen, K.M., Huang, Y., Norman, A. and Yerramille, Y., (1996). EMwave life-detection system for post-earthquake rescue operation-field test and modifications. In *Proc. 1996 IEEE/APS-URSI Int. Symp.*, Baltimore, MD, USA. 35–37.

- Chen, K.M., Huang, Y., Zhang, J. and Norman, A., (2000). Microwave life-detection systems for searching human subjects under earthquake rubble and behind barrier. *IEEE Trans. Biomed. Eng.* 27, 105–114.
- Clegg, D. Barker, R. (2004), *Case Method Fast-Track: A RAD Approach*. Addison-Wesley.
- CONSORTIS project (2014). Project ID: 312745, Funded under: FP7-SECURITY, SEC-2012.3.4-5 - Further research and pilot implementation of Terahertz detection techniques (T-Ray) - Capability Project, EU-CORDIS Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/111494_en.html [Accessed 11 Oct. 2016].
- Cordis.europa.eu, (2016a). Cordis Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/202685_en.html [Accessed 11 Oct. 2016].
- Cordis.europa.eu, (2016b). Cordis Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/88217_en.html [Accessed 11 Oct. 2016].
- Costhelper Inc. 2016. Cost of an EEG - Consumer Information - CostHelper. [online] Available at: <http://health.costhelper.com/eeg.html>. [Accessed 30 Nov, 2016].
- Council of European Union. (2004). Council Directive 2004/82/EC. *Official Journal of the European Union*, 261, 24-27.
- Council of the European Union . (2000). "Eurodac" system. Retrieved October 12, 2016, from <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l33081&from=PL>
- Council of the European Union . (2016, October 11). PRADO - Public Register of Authentic travel and identity Documents Online. Retrieved October 12, 2016, [online] Available at: <http://www.consilium.europa.eu/prado/EN/prado-start-page.html> [Accessed 19 Dec. 2016].
- Cubic and UCSD, (2015), *Envision 2020*, White paper.
- Dermalog.com, (2016). Dermalog Official Website. [online] Available at: http://www.dermalog.com/en/products_solutions/government/ [Accessed 07 Oct. 2016].
- Delloitte, (2014), *Smart Borders: Increasing security without sacrificing mobility*.
- Dhillon, H.S. Andrews, J.G. (2014). Downlink Rate Distribution in Heterogeneous Cellular Networks under Generalized Cell Selection," in *IEEE Wireless Communications Letters*, vol. 3, no. 1, pp. 42-45, doi: 10.1109/WCL.2013.110713.130709
- Digital Video Broadcasting (DVB), (2009a) *Interaction Channel for Satellite Distribution Systems*, European Telecommunication Standardization Institute (ETSI) EN 301 790 V1.4.1.
- Digital Video Broadcasting (DVB), (2009b); *Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2)*, ETSI EN 302 307,V1.2.1.
- Digital Video Broadcasting (DVB), (2010) *Second Generation DVB Interactive Satellite System (RCS2), Part 2: Lower Layers for Satellite Specification Standard*, DVB Bluebook A155-2.
- Digital Video Broadcasting (DVB), (2013) *Second Generation DVB Interactive Satellite System (DVB-RCS2), Part 1*, January 2013.
- Duan, X., Cheng, J., Zhang, L., Xing, Y., Chen, Z. and Zhao, Z., (2009). X-ray cargo container inspection system with few-view projection imaging. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 598(2), 439–444.

EFFISEC project (2009). Project ID: 217991, Funded under: FP7-SECURITY, SEC-2007-3.2-03 - Integrated check points security - Collaborative Project, EU-CORDIS Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/90955_en.html [Accessed 11 Oct. 2016].

Effisec.reading.ac.uk, (2016). Effisec -project Official Website. [online] Available at: <http://www.effisec.reading.ac.uk/project.htm> [Accessed 11 Oct. 2016].

Ekman, P., (1981). Mistakes when deceiving. *Annals of the New York Academy of Sciences*, 364(1), 269-278.

Ekman, P., (2016). Paul Ekman International Plc. [online] Available at: <http://www.ekmaninternational.com/> [Accessed 18 December 2016].

Eriksson, A. and Lacerda, F., (2007). Charlatanry in forensic speech science: A problem to be taken seriously. *International Journal of Speech, Language and the Law*, 14(2), 169-193.

Erman, A., Grapow, H., & Erichsen, W. (1950). *Wörterbuch der aegyptischen Sprache*. Berlin: JC Hinrichs.

EUR-Lex. (2016, August 23). Combating document fraud: FADO image-archiving system. [online] Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l33075> [Accessed Retrieved 12 Oct. 2016].

European Parliament . (2016). Smart Borders: EU Entry/Exit System. Brussels: European Parliament.

European Commission - Fact Sheet, (2016), Smart Borders Package: Questions & Answers.

Farah, M.J., Hutchinson, J.B., Phelps, E.A. and Wagner, A.D., (2014). Functional MRI-based lie detection: scientific and societal challenges. *Nature Reviews Neuroscience*, 15(2), 123-131.

Fastpass-project.eu, (2016). Fastpass-project Official Website. [online] Available at: <https://www.fastpass-project.eu/> [Accessed 11 Oct. 2016].

Felber, F., (2015). Demonstration of novel high-power acoustic through-the-wall sensor. In *Proc. SPIE 9456, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement XIV*, Baltimore, Maryland, USA, April 20-22. 945603 (May 14, 2015); doi:10.1117/12.2084056.

Fenton, M. Bieman, J. *Software Metrics: A Rigorous and Practical Approach*, Third Edition (Chapman & Hall/CRC Innovations in Software Engineering and Software Development Series), CRC Press; 2014.

Fingerprints and Other Biometrics. FBI (Federal Bureau of Investigation) official website. [online] Available at: <https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics> [Accessed 11, Oct. 2016].

Flesch, R. (1948) A new readability yardstick. *Journal of Applied Psychology*, 32(3), pp.221-233.

Flesch, R. (1949) *The Art of Readable Writing*. New York: Harper.

Feiler, A.R. and Powell, D.M., (2016). Behavioral expression of job interview anxiety. *Journal of Business and Psychology*, 31(1), 155-171.

Fidelity-project.eu, (2016). Fidelity-project Official Website. [online] Available at: <http://www.fidelity-project.eu/page/project.php> [Accessed 11 Oct. 2016].

- Frontex. (2016). EUROSUR, [online], Available at: from <http://frontex.europa.eu/intelligence/eurosur/> [Accessed 12th Oct. 2016]
- Frontex, (2015). Best Practice Operational Guidelines for Automated Border Control (ABC) Systems.
- Gamble, T.D., (2002). Apparatus and method for human presence detection in vehicles. U.S. Patent 6 370 481, Apr. 9, 2002.
- Gasdata.co.uk, (2016). GASDATA Gas Analysis and Control Official Website. [online] Available at: <http://www.gasdata.co.uk/products/stowaway-detector/> [Accessed 07 Oct. 2016].
- Geovox Onex, (2015). ONEX SA White Paper about Heartbeat Detector: HUMAN PRESENCE DETECTION SYSTEM, [online], Available at: <http://www.geovox.com/introAVIAN.htm> Photos retrieved from <http://www.geovox.com/introAVIAN.htm> [Accessed March 2015].
- Gemalto.com, (2016). Gemalto Official Website. [online] Available at: <http://www.gemalto.com/govt/coesys/eborder-management> [Accessed 07 Oct. 2016].
- Goldberg, C. (2016). Decimation in the Roman Republic. *The Classical Journal*, 111(2), 141-164.
- Google (no date) Google translate. Available at: <https://translate.google.co.uk/> (Accessed: 19 December 2016).
- Gosh, A. Wolter, D. R. Andrews, J, W Chen, R (2005) 'Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential', *IEEE Communications Magazine*, 129-136.
- Gotsis, A.G. Panagopoulos, A.D. Stefanatos, S. Alexiou, A. (2016) *Radio Resources Management and Optimization in 5G Networks*, "Signal Processing for 5G: Algorithms and Implementations, Wiley-IEEE Press.
- Grubin, D., (2008). The case for polygraph testing of sex offenders. *Legal and Criminological Psychology*, 13(2), 177-189
- Habermas, J., & Ciaran, C. (1998). On the past and future of sovereignty and citizenship. *Public Culture*, 10(2), 397-416.
- HANDHOLD project (2012). Project ID: 284456, Funded under: FP7-SECURITY, SEC-2011.3.4-2 - "Artificial sniffer"- Capability Project, EU-CORDIS Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/102760_en.html. [Accessed 19 Dec. 2016].
- Honts, C.R. and Reavy, R., (2015). The comparison question polygraph test: A contrast of methods and scoring. *Physiology & behavior*, 143, 15-26.
- Herms, R., (2016). Prediction of Deception and Sincerity from Speech using Automatic Phone Recognition-based Features. *Interspeech 2016*, pp.2036-2040.
- Huguenin, G.R. (1997). Millimeter-wave concealed weapons detection and through-the-wall imaging systems. *Proceedings of SPIE - The International Society for Optical Engineering*
- IEEE Biometrics Compendium. IEEE (Institute of Electrical and Electronics Engineers) official website. [online] Available at: http://www.ieee.org/publications_standards/publications/subscriptions/prod/biometricscompendium.html [Accessed Oct. 2016].
- Information Centre of Ministry of Interior of the Republic of Latvia. 2012. Register of Document Samples. [online] Available at: <http://www.ic.iem.gov.lv/en/node/403>. [Accessed 18 Dec. 2016].

The International Rail Transport Committee. 2015. General Conditions of Carriage for Rail Passengers. [online] Available at: http://www.cit-rail.org/files/Documentation_EN/Passenger/GCC_CIV_PRR/GCC_CIV-PRR_EN_2015-10-01.pdf?cid=570. [Accessed 18 Dec. 2016].

International law - Library of Congress. 2005. [online]. Available: <http://www.loc.gov/catdir/samples/cam041/2003051552.pdf>, [Accessed 23 Sep. 2016].

ION Sensor, (2016). ION Sensor SM-24 Geophones. ION Sensor Inc. Product online brochure, [online], Available at: www.iongeo.com/.../BR_SEN_Geophones_091509.pdf; [Accessed 12 Oct. 2016].

Iris.com, (2016). Iris Official Website. [online] Available at: http://www.iris.com.my/Trusted_ID/product_03document.html [Accessed 07 Oct. 2016].

Jain, A., Flynn, P., Ross, A., A Handbook of Biometrics.. ISBN 978-0-387-71041-9. Springer

Ji, Q., B. Moeslund, Th., Hua, G., Nasrollahi, K (2014) Face and Facial Expression Recognition from Real World Videos. ISBN 978-3-319-13737-7.

Jones, C. (n.d.). EU: Secretive Frontex Working Group seeks to increase surveillance of travellers, [online], Available at: <http://www.statewatch.org/analyses/no-217-frontex-traveller-surveillance> [Accessed 12 Oct. 2016].

Justice and home affairs . (2016, June 01). EU Passenger Name Record (PNR) directive: an overview. [online], Available at: [http://www.europarl.europa.eu/news/en/news-room/20150123BKG12902/eu-passenger-name-record-\(pnr\)-directive-an-overview](http://www.europarl.europa.eu/news/en/news-room/20150123BKG12902/eu-passenger-name-record-(pnr)-directive-an-overview) [Accessed 12 Oct. 2016].

Kaushik Roy, Prabir Bhattacharya (2008). Iris Recognition: A Machine Learning Approach. ISBN 978-3639082593.

Keesingtechnologies.com, (2016). Keesingtechnologies Official Website. [online] Available at: <https://www.keesingtechnologies.com/automated-id-checking/premium/> [Accessed 07 Oct. 2016].

Kincaid, J. P., Fishburne, R. P, Rogers, R. L. and Chissom, B. S. (1975) Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel. Virginia: National Technical Information Service. (RBR 8-75).

Kirkendall, B., Li, Y. and Oldenburg, D., (2007). Imaging Cargo Containers Using Gravity Gradiometry. *IEEE Trans. On Geoscience and Remote Sensing* 45(6), 1786-1797.

Klock, B.A., (2006). Selected Systems for the Detection of Human Stowaways in Air Cargo Containers. Proceedings 40th Annual IEEE International Carnahan Conference on Security Technology, Kentucky, USA, October 16-19.

Kokish, R., Levenson, J.S. and Blasingame, G.D., (2005). Post-conviction sex offender polygraph examination: Client-reported perceptions of utility and accuracy. *Sexual Abuse: A Journal of Research and Treatment*, 17(2), 211-221.

Konopka, C., Wurzbach, J.A. and Silvia, M.T., (2012). Methods and apparatus for using acoustic inspection of containers to image objects. U.S. Patent 9 459 238, Mar 13, 2012.

Kourogorgas, C. Panagopoulos, A.D. Makri, R. (2017) A Copulas-Based Time Series Synthesizer for Mobile Satellite Communications Operating Above 10 GHz, EUCAP 2017, Paris, March, 2017, *in press*.

Kresimir Delac and Mislav Grgic (2007) Face Recognition. ISBN 978-3-902613-03-5

Kyritsis, Al., (2016). Active and Passive Methods for Detecting small unmanned aerial objects. Diploma Thesis, National Technical University of Athens, July 2016, Supervisors: N.K. Uzunoglu, R. Makri.

Lafayette Polygraph (2016) [online] Available at:
http://lafayettepolygraph.com/product_detail.asp?itemid=1225 [Accessed 23 Oct. 2016].

Lanfermann, F. (2014). The European Union's Border Management. A study about the coordination in its horizontal and vertical dimension. Lund: Lund University Publishing.

Lawrence Rabiner, Bing-Hwang Juang (1993) Fundamentals of Speech Recognition. ISBN 978-0130151575

Lie Detectors UK (2016). [online] Available at: <https://liedetectors-uk.com/pages/faq/#toggle-id-4> [Accessed 23 Oct. 2016]

Lin, J.C., (1992). Microwave sensing of physiological movement and volume change: A review. *Bioelectromagnetics*. 13(6), 557–565.

Lawson, G., Stedmon, A.W., Zhang, K., Eubanks, D.L. and Frumkin, L.A., (2013). The effects of self-awareness on body movement indicators of the intention to deceive. *Applied ergonomics*, 44(5), 687-693.

Leidos.com, (2016). Leidos Official Website. [online] Available at:
<https://www.leidos.com/products/security/vacis-ip6500-fullscan/> [Accessed 07 Oct. 2016].

Liu, Y., Sowerby, B.D. and J.R. Tickner, (2008). Comparison of neutron and high-energy X-ray dual-beam radiography for air cargo inspection. *Applied Radiation and Isotopes*, 66(4), 463-473.

Li, X., Pfister, T., Huang, X., Zhao, G. and Pietikäinen, M., (2013), April. A spontaneous micro-expression database: Inducement, collection and baseline. 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition, 1-6.

Levitan, S.I., Levine, M., Hirschberg, J., Cestero, N., An, G. and Rosenberg, A., 2015. Individual differences in deception and deception detection. In the Seventh International Conference on Advanced Cognitive Technologies and Applications.

Levitan, S.I., An, G., Ma, M., Levitan, R., Rosenberg, A. and Hirschberg, J., (2016). Combining Acoustic-Prosodic, Lexical, and Phonotactic Features for Automatic Deception Detection. *Interspeech 2016*, 2006-2010.

Lyngsat Maps: [online]. Available: <http://www.lyngsat-maps.com/footprints/Eutelsat-Hot-Bird-13C-Wide.html>. [Accessed 06 Dec.2016]

Mangan, D.J., Armitage, T.E. and Adams, G.C., (2008). A field study on the validity of the Quadri-Track Zone Comparison Technique. *Physiology & behavior*, 95(1), 17-23.

Mária, T. D. (2007). Az államhatár rendjének jogi védelme az EU-csatlakozás tükrében: doktori (PhD) értekezés.

Meijer, E.H., Verschuere, B., Gamer, M., Merckelbach, H. and Ben-Shakhar, G., (2016). Deception detection with behavioral, autonomic, and neural measures: Conceptual and methodological considerations that warrant modesty. *Psychophysiology*.

MFI Medical. 2016. Cadwell Easy II EEG/PSG System - MFI Medical. [online] Available at: <https://mfimedical.com/collections/eeg-ltm-psg-systems-accessories/products/cadwell-easy-ii-eeg-psg-system>. [Accessed 30 Nov. 2016].

Microsoft (2016) Bing translator. Available at: <https://www.bing.com/translator> (Accessed: 19 December 2016).

Migration and Home Affairs. (2015, December 16). Schengen Information System., [online], Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm [Accessed 12 Oct., 2016].

Migration and Home Affairs. (2015, June 23). Visa Information System (VIS), [online], Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm [Accessed 12 Oct., 2016].

Mobilepass-project.eu, (2016). Mobilepass-project Official Website. [online] Available at: <http://mobilepass-project.eu/> [Accessed 11 Oct. 2016].

Moravcsik, A., & Nicolaïdis, K. (1999). Explaining the Treaty of Amsterdam: interests, influence, institutions. JCMS: Journal of Common Market Studies, 37(1), 59-85.

Morpho.com, (2016). Morpho Official Website. [online] Available at: <http://www.morpho.com/en/public-security/check-id/document-authentication/b5000> [Accessed 07 Oct. 2016].

Nalini K. Ratha BTech, MTech, PhD, Venu Govindaraju BTech, MS, PhD (2008) Advances in Biometrics. ISBN: 978-1-84628-920-0

Narayanan, R.M., Smith, S. and Gallagher, K.A. (2014). A Multi-frequency Radar System for Detecting Humans and Characterizing Human Activities for Short-Range Through-Wall and Long-Range Foliage Penetration Applications. International Journal of Microwave Science and Technology, Vol. 2014.

NASA JPL, (2015 April). Article of Media Contact [online], Elizabeth Landau, NASA's Jet Propulsion Laboratory, Pasadena, Calif. USA. Available at: <http://www.jpl.nasa.gov/news/news.php?feature=4578> [Accessed 19 Dec. 2016].

New York State Department of Environmental Conservation (2014, April 14). K9 Unit: Duties and Responsibilities, [online], Available at: https://en.wikipedia.org/wiki/Police_dog [Accessed 12 Oct. 2016].

N. Shaw, M. (2003). International Law (5 ed.). Cambridge: Cambridge University Press, [online], Available at: <http://www.loc.gov/catdir/samples/cam041/2003051552.pdf> [Accessed 23 Sept. 2016].

NHS. 2015. Electroencephalogram (EEG) - NHS Choices. [online] Available at: <http://www.nhs.uk/Conditions/EEG/Pages/Introduction.aspx>. [Accessed 30 Nov. 2016].

No Lie MRI. 2006. No Lie MRI - Test Centers. [online] Available at: <http://www.noliemri.com/centers/Centers.htm>. [Accessed 30 Nov. 2016].

O'Gorman, K. D. (2010). Introduction to The origins of hospitality and tourism. Oxford: Goodfellow.

Oppenheim, A. (1998) Questionnaire Design, Interviewing and Attitude Measurement, Continuum-3PL; New edition, 1998, ISBN-10: 0826451764, ISBN-13: 978-0826451767

Origins-project.eu, (2016). Origins-project. Official Website. [online] Available at: <http://www.origins-project.eu/> [Accessed 11 Oct. 2016].

OTIF (Intergovernmental Organisation for International Carriage by Rail). 1999. COTIF 1999 Convention concerning International Carriage by Rail. [online] Available at: http://www.otif.org/fileadmin/user_upload/otif_verlinkte_files/04_recht/03_CR/03_CR_24_NOT/COTIF_1999_01_12_2010_e.pdf. [Accessed 18 Dec. 2016].

Panagopoulos, A.D. (2015) Propagation Phenomena and Fade Mitigation Techniques for Fixed Satellite Systems”, Book Chapter in the Book “Radio Wave Propagation and Channel Modelling for Earth-Space Systems”, CRC Press.

Péter, T. (1997). Az állam fogalma. In T. Péter (Ed.), Államelmélet. Előadások az államelmélet és az állambölcsélet köréből. (pp. 9-28.). Miskolc: Bíbor Kiadó.

International League of Polygraph Examiners (2016), Polygraph/Lie Detector FAQs. [online]. Available at: http://www.theilpe.com/faq_eng.html. [Accessed 23 Oct. 2016]

Papafragkakis, A.Z. Panagopoulos, A.D. (2015) Machine-to-machine communication systems: converged architectures, services and interference evaluation, Nova Publications.

Poulakis, M. Vassaki, S. Kourogioras, C. Pitsiladis, G. Panagopoulos, A.D. Gardikis, G. Costicoglou, S. (2014). Use of Satellite Communication Systems and Services for Monitoring of Critical Infrastructures and Safety Applications, in Proc. of 20th Ka Conference.

Porter, S., Ten Brinke, L. and Wallace, B., (2012). Secrets and lies: Involuntary leakage in deceptive facial expressions as a function of emotional intensity. *Journal of Nonverbal Behavior*, 36(1), 23-37.

Rao, E., (2012). Air cargo screening for stowaway detection: Carbon dioxide monitors and Heartbeat Monitor assessment and qualification. 2012 IEEE International Carnahan Conference on Security Technology (ICCST), Boston, USA, October 15-18.

Rapiscansystems.com, (2016). Rapiscan Systems Official Website. [online] Available at: <http://www.rapiscansystems.com/en/products> [Accessed 07 Oct. 2016].

Regulaforensics.com, (2016). Regulaforensics Official Website. [online] Available at: <https://regulaforensics.com/en/> [Accessed 07 Oct. 2016].

Reynolds, J.M. (2011). An Introduction to Applied and Environmental Geophysics-second edition. WILEY BLACKWELL. p. 170. ISBN 978-0-471-48535-3.

Roberts, W. (2001), Traffic theory and the Internet, in *IEEE Communications Magazine*, vol. 39, no. 1, pp. 94-99.

Rogers, T.W., Jaccard, N., Morton, E.J. and Griffin, L.D., (2016). Automated X-ray Image Analysis for Cargo Security: Critical Review and Future Promise. *Journal of X-ray Science and Technology*.

Roman, D., Thompson, K., Ernst, L. and Hakuta, K., (2016), WordSift: A free web-based vocabulary tool designed to help science teachers in integrating interactive literacy activities. *Science Activities: Classroom Projects and Curriculum Ideas*, 53(1), pp.13-23.

Rosenfeld, J.P., Hu, X., Labkovsky, E., Meixner, J. and Winograd, M.R., (2013). Review of recent studies and issues regarding the P300-based complex trial protocol for detection of concealed information. *International Journal of Psychophysiology*, 90(2), 118-134.

- Rothwell, J., Bandar, Z., O'Shea, J. and McLean, D., 2006. Silent talker: a new computer-based system for the analysis of facial cues to deception. *Applied cognitive psychology*, 20(6), 757-777.
- Sabloff, J. A. (1975). *Ancient civilization and trade*. Albuquerque: New Mexico University Press.
- Sadasivan, S., Gurubasavaraj, M., Sekar, S.R. et al., (2001). Acoustic Signature of an Unmanned Air Vehicle – Exploitation for Aircraft Localization and Parameter Estimation. *Defence Science Jnl.* 51(3), 279-284.
- Sagkriotis, S.E. Panagopoulos, A.D. (2016). Optimal FFR Policies: Maximization of Traffic Capacity and Minimization of Base Station's Power Consumption, in *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 40-43, doi: 10.1109/LWC.2015.2491943
- Sallai, J. (2004). *Az államhatárok*. Budapest: Press Publica.
- Saxe, L., Dougherty, D. and Cross, T., (1985). The validity of polygraph testing: Scientific analysis and public controversy. *American Psychologist*, 40(3), 355.
- Savran, A., Alyüz, N., Dibeklioglu, H., Çeliktutan, O., Gökberk, B., Sankur, B. and Akarun, L., (2008). Bosphorus Database for 3D Face Analysis, Biometrics and Identity Management: First European Workshop, BIOID 2008, Roskilde, Denmark, May 7-9. *Selected Papers*.
- Semlex.com, (2016). Semlex Official Website. [online] Available at: <http://www.semlex.com/en/products/border-management/> [Accessed 07 Oct. 2016].
- Shi, X. and Yang, M.H. (2014). Development of passive millimeter wave imaging for concealed weapon detection indoors. *Microwave and Optical Technology Letters*. 56(7), 1701–1706.
- Shi, W., Arabadjis, G., Bishop, B., Hill, P., Plasse, R. and Yoder, J., (2011). Detecting, Tracking, and Identifying Airborne Threats with Netted Sensor Fence. The MITRE Corporation Bedford, Massachusetts, U.S.A, Chapter in Book: “Sensor Fusion - Foundation and Applications”, Dr. Ciza Thomas (Ed.), ISBN: 978-953-307-446-7, InTech
- Siemens Healthcare Limited. 2016. MAGNETOM Prisma - MRI Scanner - Siemens Healthineers United Kingdom. [online] Available at: <https://www.healthcare.siemens.co.uk/magnetic-resonance-imaging/3t-mri-scanner/magnetom-prisma/technical-details>. [Accessed 30 Nov. 2016].
- Smithsdetection.com, (2016). Smiths Detection Official Website. [online] Available at: <http://www.smithsdetection.com> [Accessed 07 Oct. 2016].
- SNOOPY project (2014). Project ID: 313110, Funded under: FP7-SECURITY, SEC-2012.3.4-4 - Innovative, cost-efficient, and reliable technology to detect humans hidden in vehicles/closed compartments - Capability Project, EU-CORDIS Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/111313_en.html [Accessed 07 Oct. 2016].
- SNIFFER project (2012). Project ID: 285203, Funded under: FP7-SECURITY, SEC-2011.3.4-2 - “Artificial sniffer”- Capability Project, EU-CORDIS Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/102348_en.html [Accessed 07 Oct. 2016].
- SNIFFLES project (2012). Project ID: 285045, Funded under: FP7-SECURITY, SEC-2011.3.4-2 - “Artificial sniffer”- Capability Project, EU-CORDIS Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/102069_en.html [Accessed 07 Oct. 2016].
- Stout, J. F. (1975). Aggressive communication by *Larus glaucescens* III. Description of the displays related to territorial protection. *Behaviour*, 55(3), 181-207.

- Study.com. 2016. EEG Technician Education, Training and Career Information. [online] Available at: http://study.com/eeg_technician.html. [Accessed 30 Nov. 2016].
- Su, L. and Levine, M., (2016). Does “lie to me” lie to you? An evaluation of facial clues to high-stakes deception. *Computer Vision and Image Understanding*, 147, 52-68.
- Supremainc.com, (2016). Supremainc Official Website. [online] Available at: <https://www.supremainc.com/en/Document-Readers/Readers/RealPass-V#> [Accessed 07 Oct. 2016].
- Tabularasa-euproject.org, (2016). Tabularasa-project Official Website. [online] Available at: <https://www.tabularasa-euproject.org/> [Accessed 11 Oct. 2016].
- Tatalovic, M. (2010). Evolution of raised guarding behavior in meerkats, *Suricata suricatta*. *Journal of Young Investigators*, 19(24), 2-8.
- TERASCREEN project (2013). Project ID: 312496, Funded under: FP7-SECURITY, SEC-2012.3.4-5 - Further research and pilot implementation of Terahertz detection techniques (T-Ray) - Capability Project, EU-CORDIS Official Website. [online] Available at: http://cordis.europa.eu/project/rcn/108442_en.html; [Accessed 11 Oct. 2016].
- The UN Refugee Agency Website (2016). [online] Available at: <https://data.unhcr.org/mediterranean/documents.php?page=1&view=grid&Country%5B%5D=83&Type%5B%5D=3>, [Accessed: 18 Dec. 2016]
- Tilly, C., & Ardant, G. (1975). *The formation of national states in Western Europe*. Princeton: Princeton University Press.
- Treadgold, W. T., & Treadgold, W. (1998). *Byzantium and its Army, 284-1081*. Stanford: Stanford University Press.
- Tribe, W.R., Newnham, D.A., Taday, P.F. and Kemp, M.C., (2004). Hidden object detection: security applications of terahertz technology. *Terahertz and Gigahertz Electronics and Photonics III*, Proc. of SPIE, Vol. 5354 (SPIE, Bellingham, WA). 168-176.
- Trovillo, P.V., (1939). A history of lie detection. *Journal of Criminal Law and Criminology* (1931-1951), 29(6), 848-881.
- Valstar, M.F. and Pantic, M., (2012) Fully automatic recognition of the temporal phases of facial actions. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 42(1), 28-43.
- Varga, J. (2015). Az Integrált Határigazgatás európai uniós rendszere. *Hadtudományi Szemle*, 8(3), 170-176.
- Vassaki, S. Pitsiladis, G. Kourogiorgas, C. Poulakis, M. Panagopoulos, A.D. Gardikis, G. and Costicoglou, S. (2014) *Satellite-Based Sensor Networks: M2M Sensor Communication and Connectivity Analysis* in Proc. of TEMU.
- Vasquez, J. R., Tarplee, K. M., Case, E. E., Zelnio, A. M., Rigling, B. D., (2008). Multisensor 3D tracking for counter small-unmanned air vehicles (CSUAV). *Proc. SPIE Vol. 6971, Acquisition, Tracking, Pointing, and Laser Systems Technologies XXII*, 697107 (2008); doi: 10.1117/12.785531, Steven L. Chodos; William E. Thompson, Editor(s).
- Vrij, A., Edward, K., Roberts, K.P. and Bull, R., (2000). Detecting deceit via analysis of verbal and nonverbal behavior. *Journal of Nonverbal behavior*, 24(4), 239-263.

Veridos.com, (2016). Veridos Official Website. [online] Available at: <https://www.veridos.com/passport-reader> [Accessed 07 Oct. 2016].

Welle, I., Berclaz, M., Lacasa, M.J. and Niveau, G., (2011). A call to improve the validity of criterion-based content analysis (CBCA): Results from a field-based study including 60 children's statements of sexual abuse. *Journal of Forensic and Legal Medicine*, 43, 111-119.

Wang, S.J., Yan, W.J., Zhao, G., Fu, X. and Zhou, C.G., (2014), September. Micro-expression recognition using robust principal component analysis and local spatiotemporal directional features. In *Workshop at the European Conference on Computer Vision*, Springer International Publishing, 325-338.

Warren, G., Schertler, E. and Bull, P., (2009). Detecting deception from emotional and unemotional cues. *Journal of Nonverbal Behavior*, 33(1), 59-69.

Whiffen, J., Naylor, M., (2005). Acoustic signal processing techniques for container security. The IEE Seminar on Signal Processing Solutions for Homeland Security, London, UK, October 11

Wikipedia (2016, May 4). Geophone. [online]. Available at: <https://en.wikipedia.org/wiki/Geophone>. [Accessed 23 Oct. 2016].

Wireless Lie Detector Polygraph, 2016 [online] Available: <http://csspakistan.com/wireless-lie-detector-polygraph/> [Accessed 23 Oct. 2016].

Walczyk JJ, Igou FP, Dixon AP, Tcholakian T. Advancing lie detection by inducing cognitive load on liars: a review of relevant theories and techniques guided by lessons from polygraph-based approaches, *Frontiers in Psychology*, 4, 01 February 2013, [online] Available at: <http://dx.doi.org/10.3389/fpsyg.2013.00014> [Accessed 23 Oct. 2016].

Wolpe, P.R., Foster, K.R. and Langleben, D.D., (2005). Emerging neurotechnologies for lie-detection: Promises and perils. *The American Journal of Bioethics*, 5(2), 39-49.

Yan, W.J., Li, X., Wang, S.J., Zhao, G., Liu, Y.J., Chen, Y.H. and Fu, X., (2014). CASME II: An improved spontaneous micro-expression database and the baseline evaluation. *PloS one*, 9(1), p.e86041.

Yin, L., Chen, X., Sun, Y., Worm, T. and Reale, M., (2008), A high-resolution 3D dynamic facial expression database. In *Automatic Face & Gesture Recognition*, 8th IEEE International Conference On FG'08, 1-6.

Zentai, G., (2008). X-ray imaging for homeland security. *IEEE International Workshop on Imaging Systems and Techniques (IST)*, Chania, Greece, September 10-12.

Zhu, Z., Hu, Y. and Zhao, L., (2010). Gamma/X-ray linear pushbroom stereo for 3D cargo inspection. *Machine Vision and Applications*, 21(4), 413-425.

8 Appendix A Travellers Questionnaire

8.1 English Template

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Age Group	Percentage Vaccinated
18-24	10%
25-34	15%
35-44	35%
45-54	95%
55-64	55%
65-74	95%
75-84	75%
85+	55%

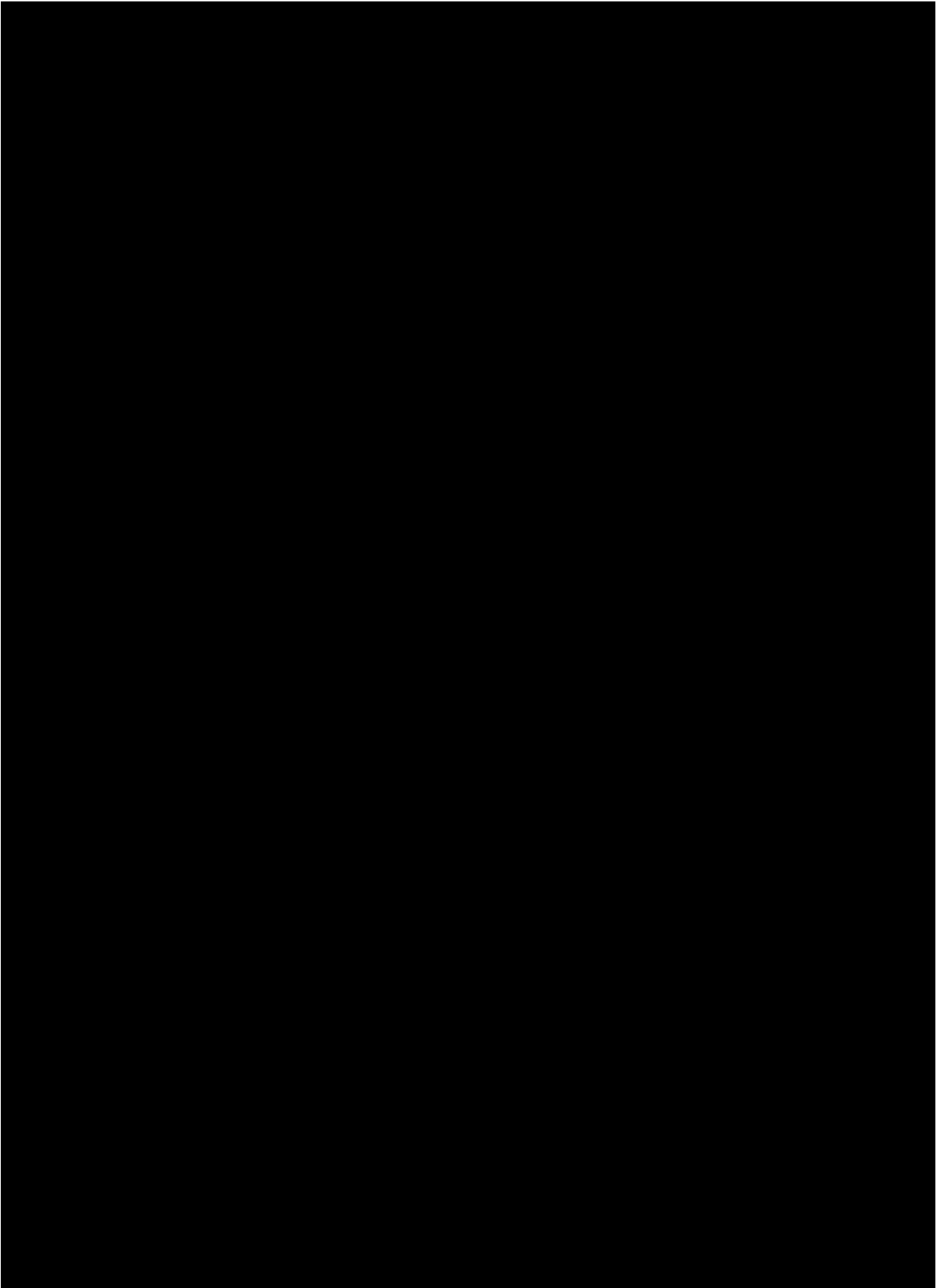
A horizontal bar chart titled 'U.S. should take action to address climate change' showing the percentage of respondents who believe the U.S. should take action to address climate change, broken down by age group. The y-axis lists age groups: 18-29, 30-49, 50-64, 65+, and All. The x-axis represents the percentage from 0 to 100. The bars show that 85% of 18-29, 71% of 30-49, 68% of 50-64, 88% of 65+, and 80% of all respondents believe the U.S. should take action to address climate change.

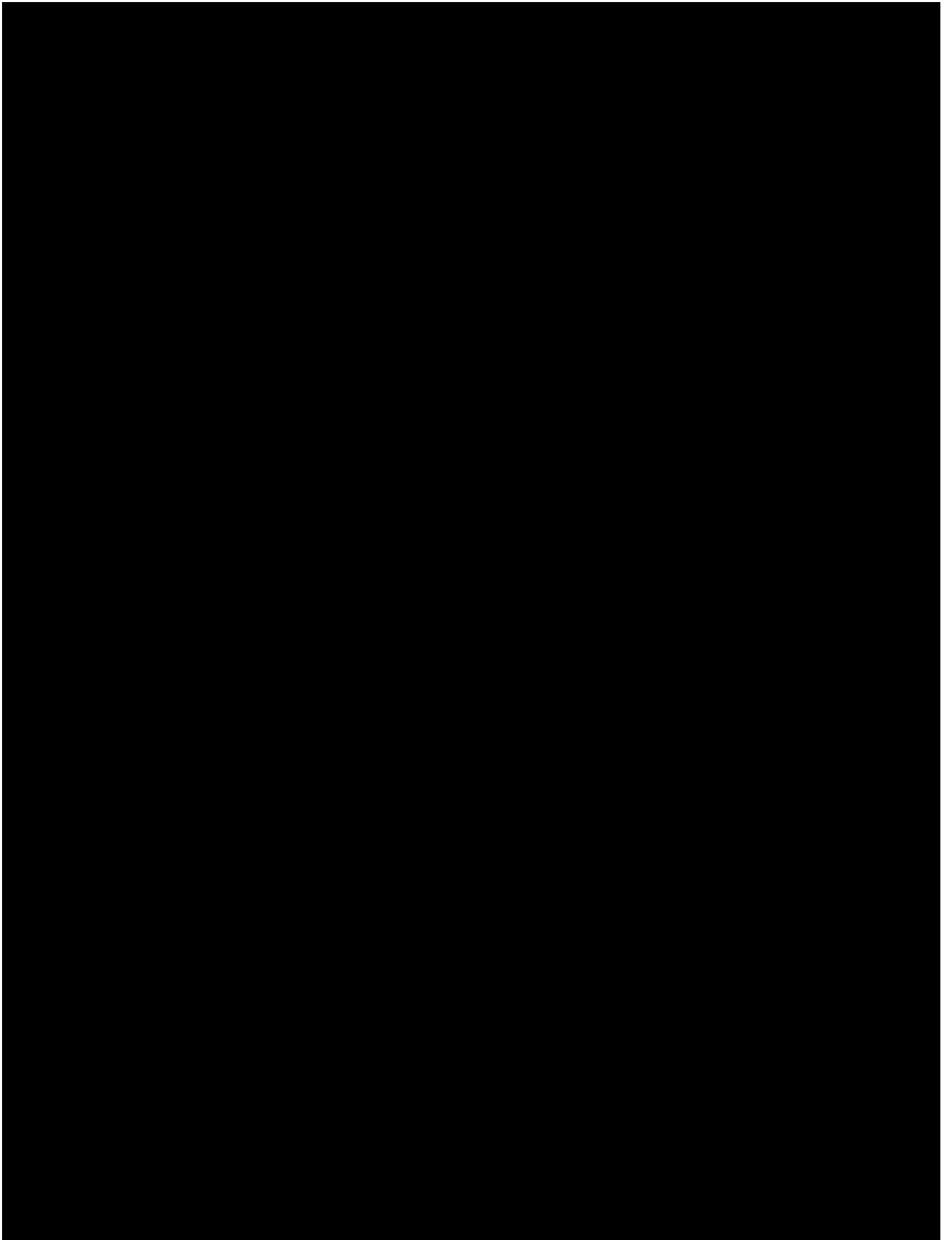
Age Group	Percentage
18-29	85%
30-49	71%
50-64	68%
65+	88%
All	80%

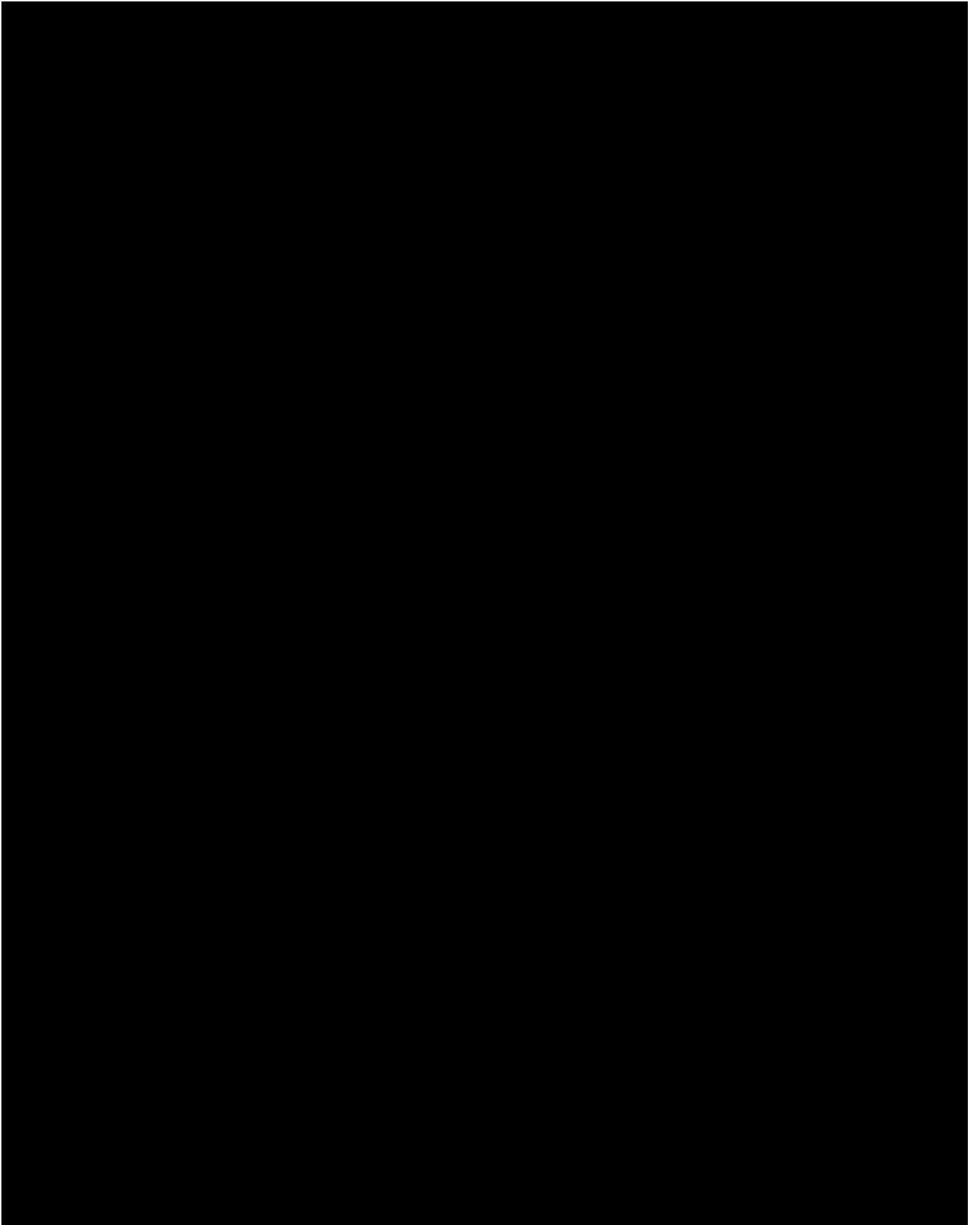
8.2 Hungarian Version

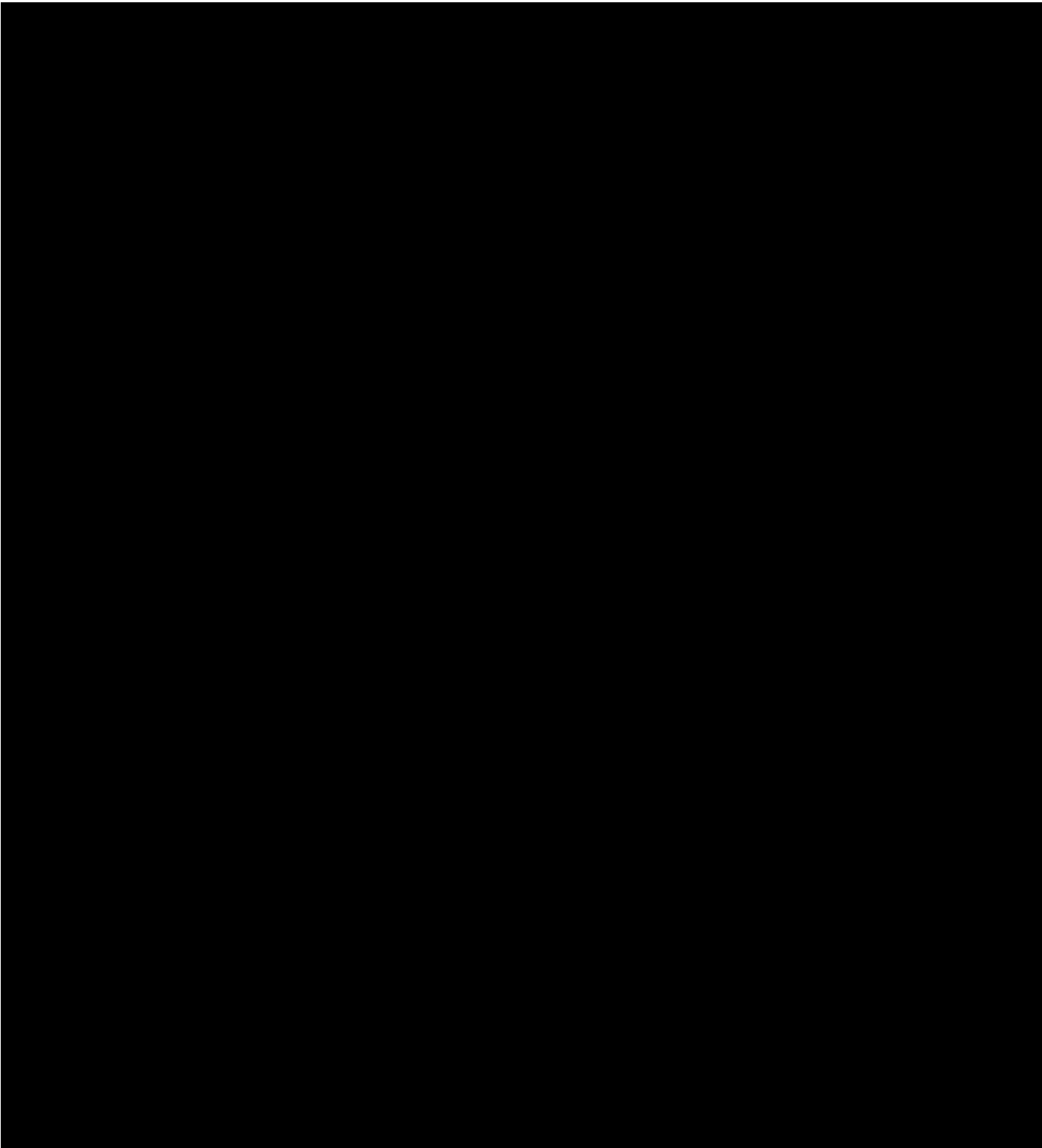
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED] [REDACTED] [REDACTED]
[REDACTED]
[REDACTED]

██████████

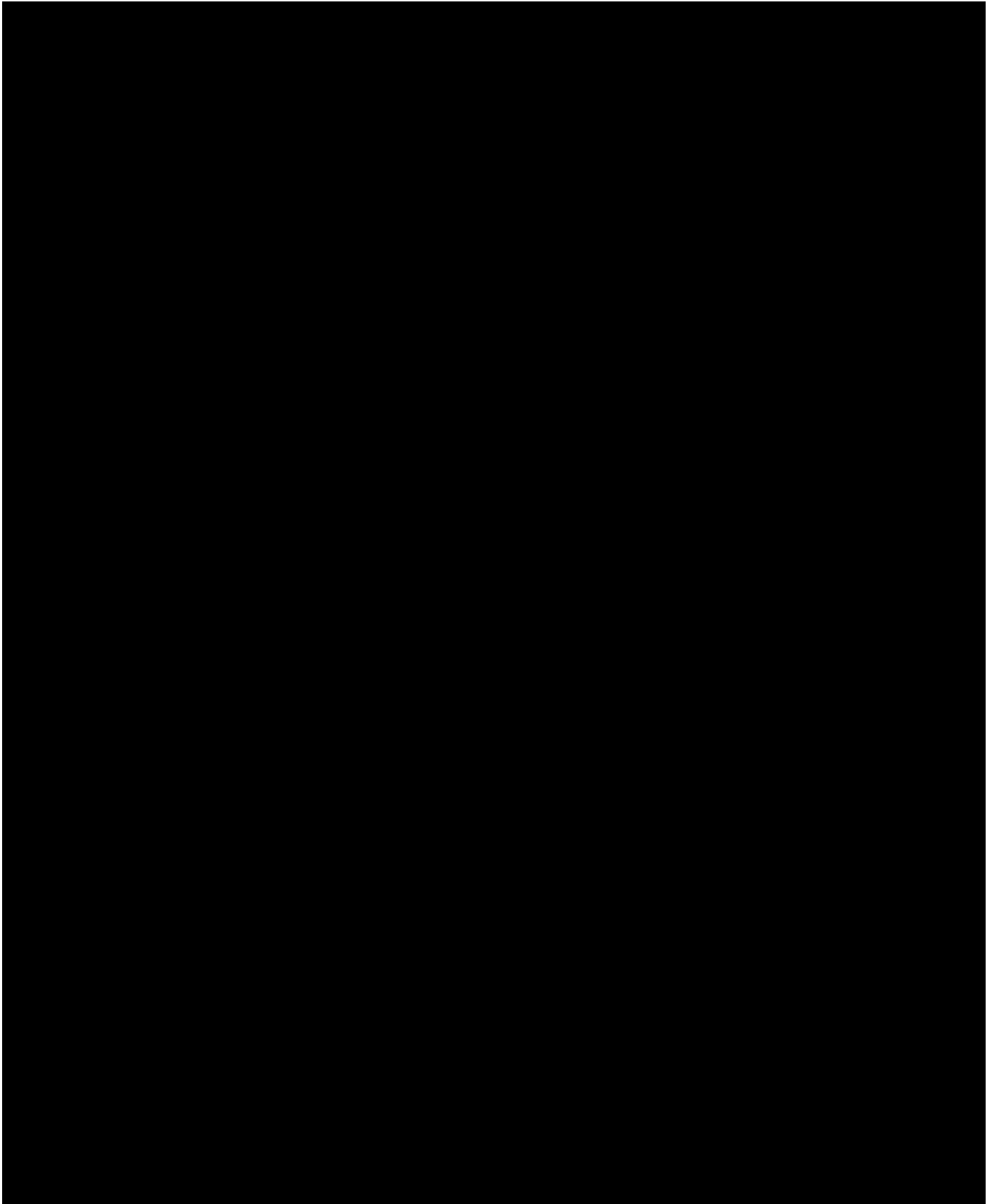


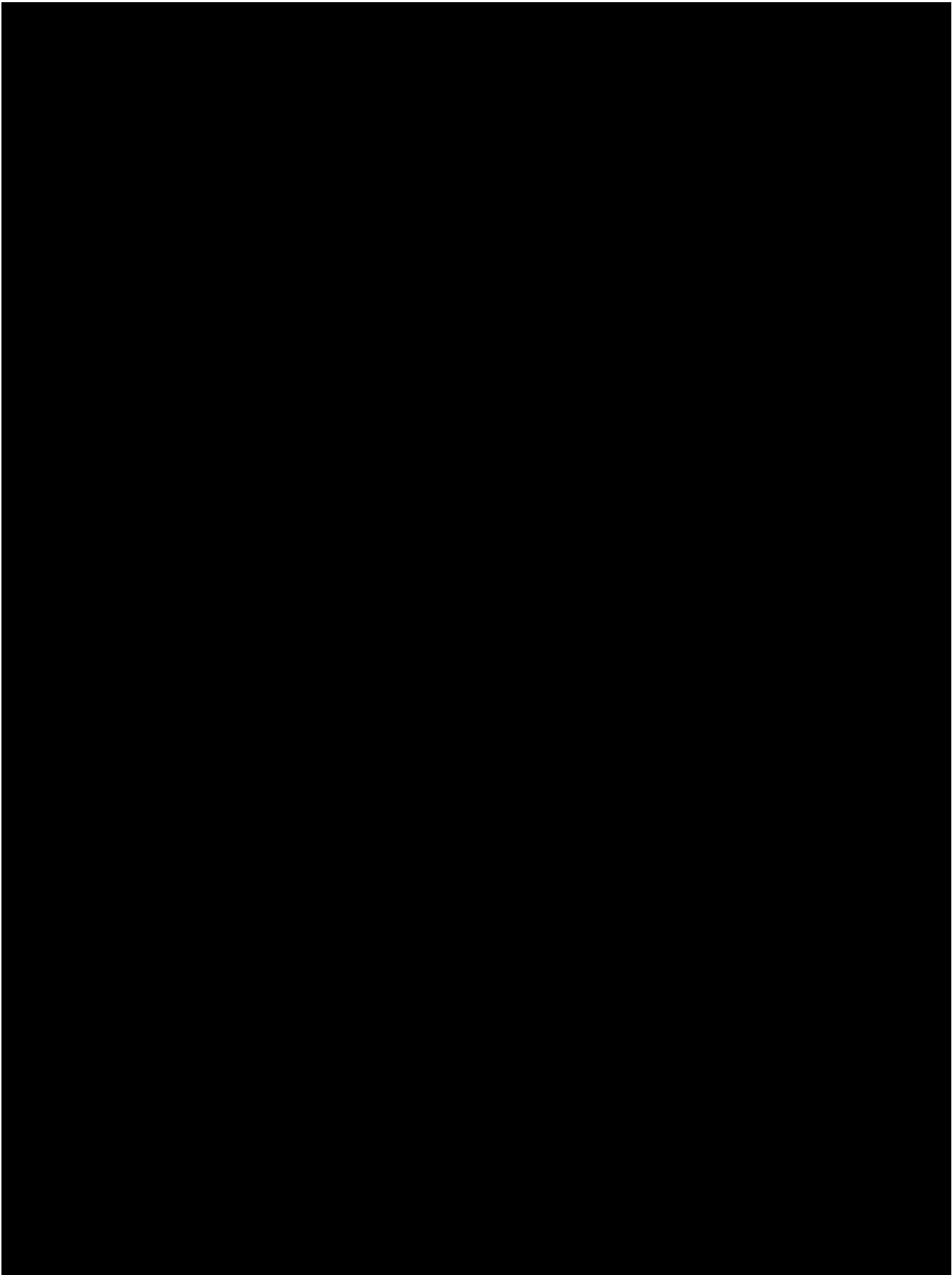


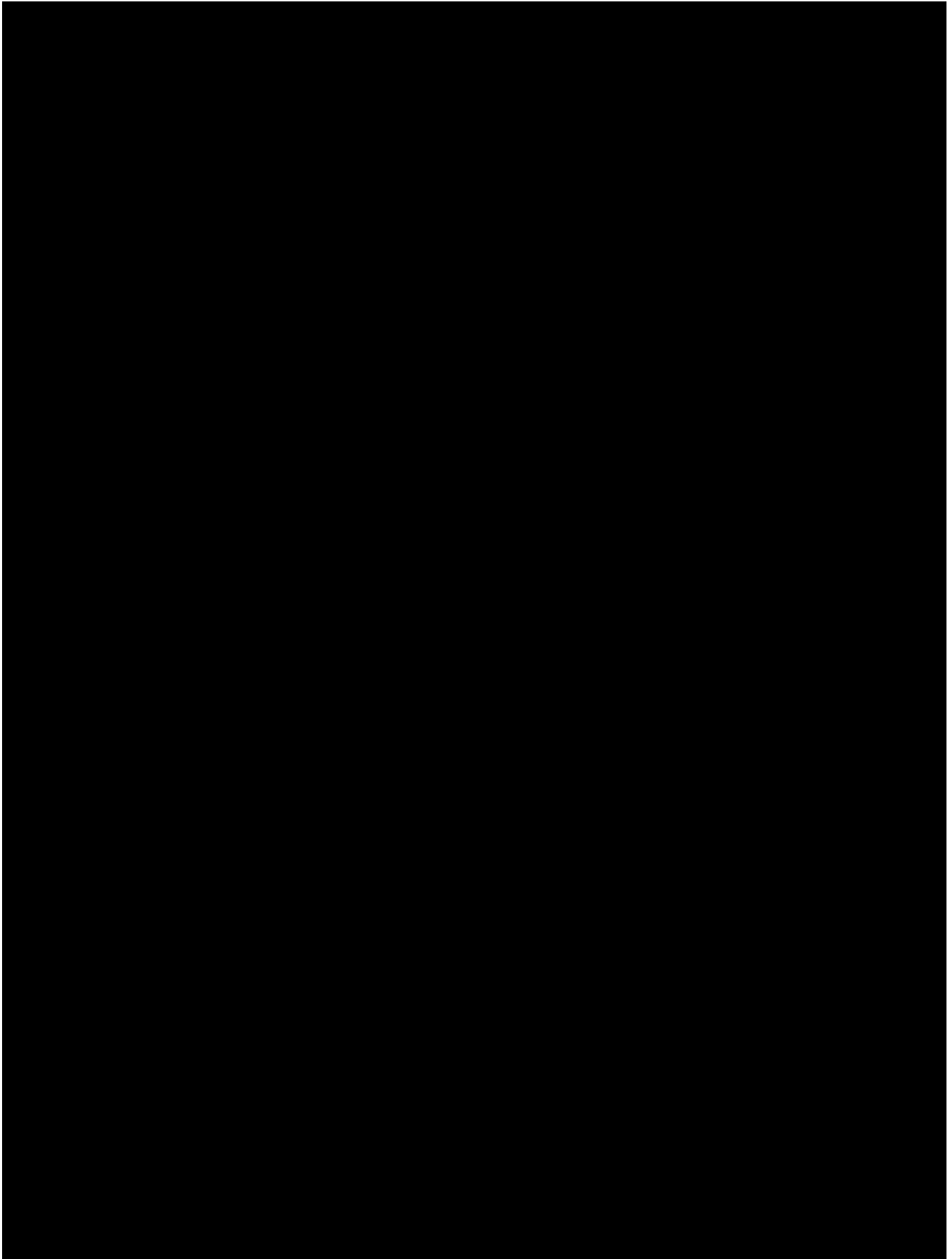


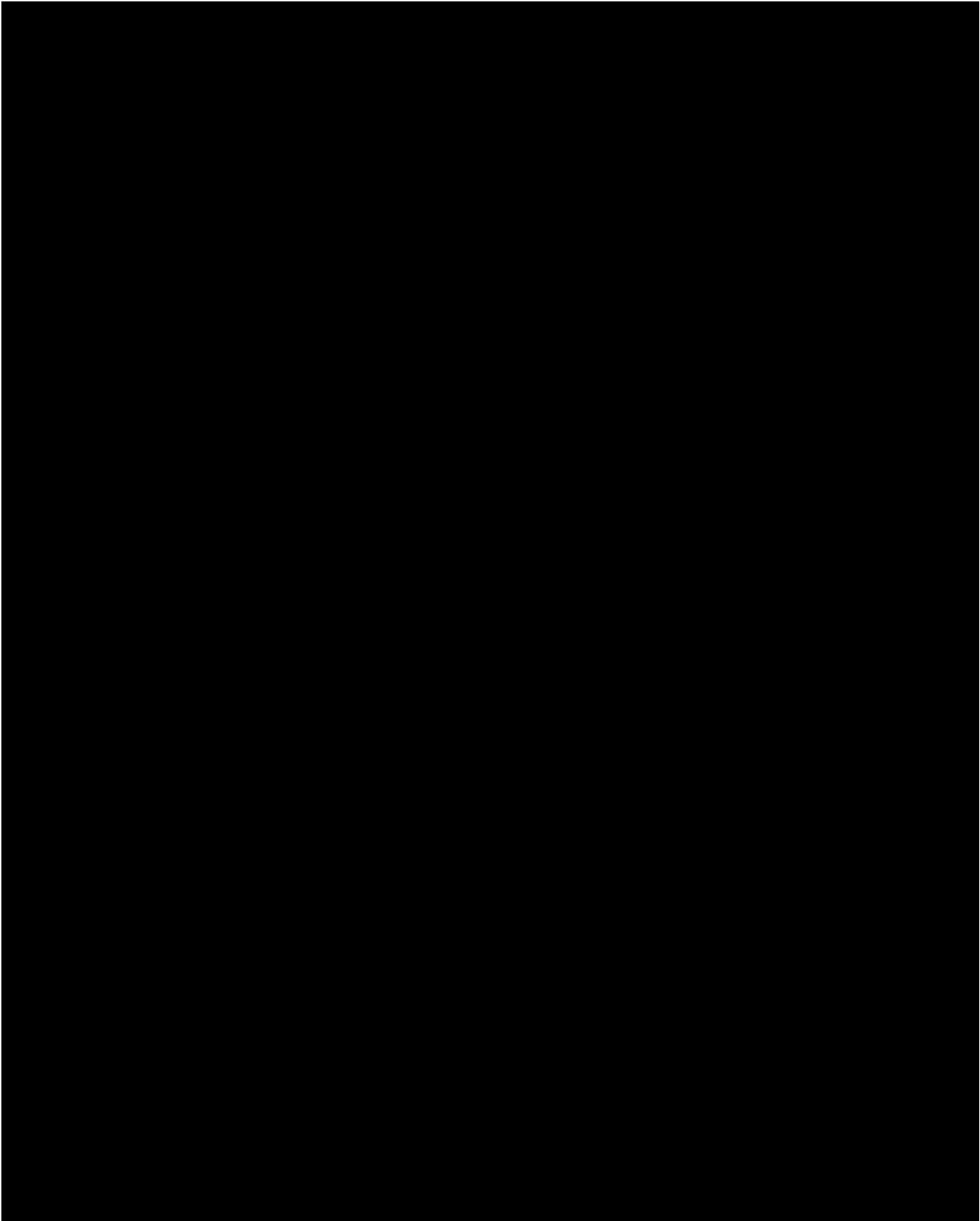


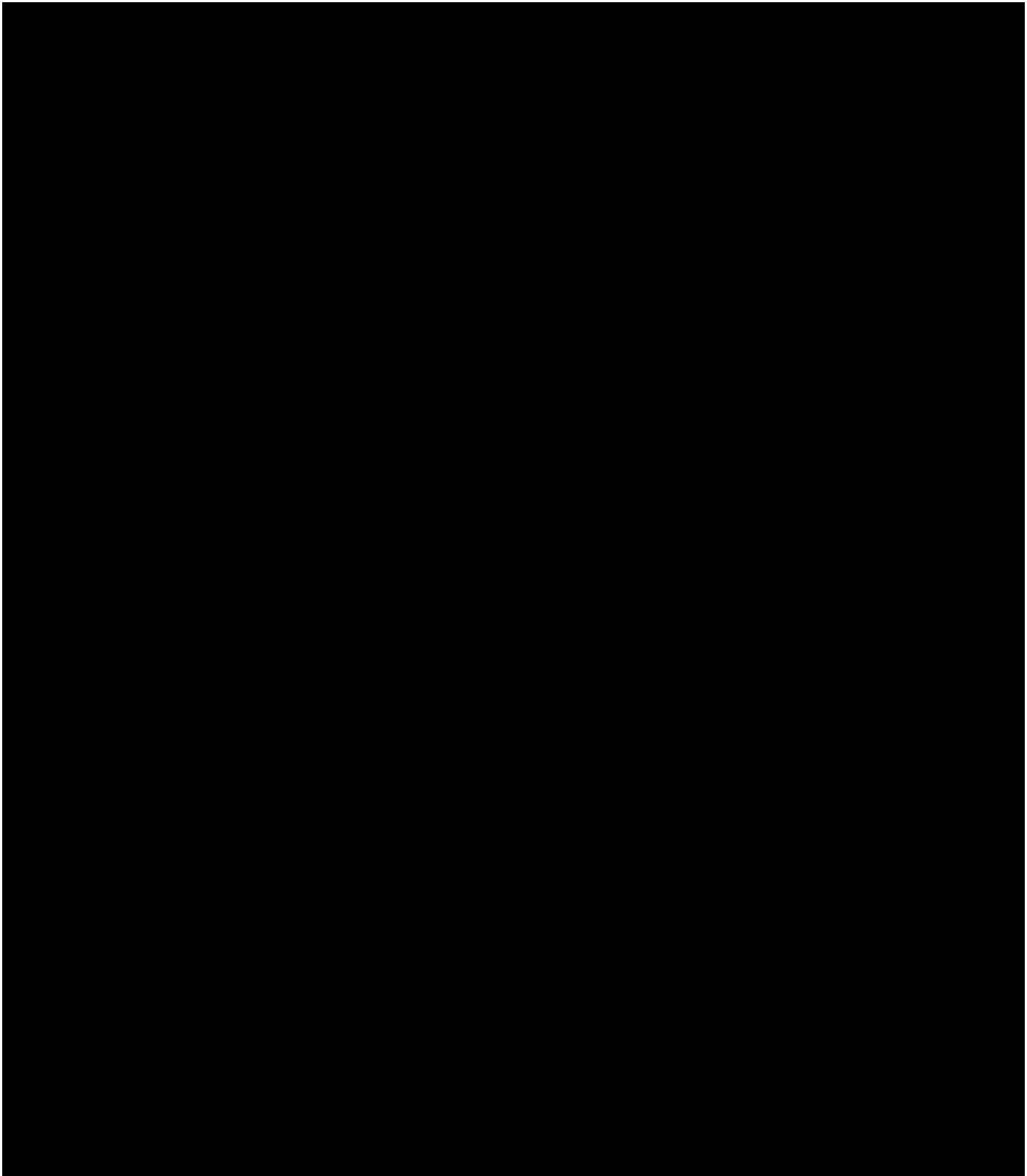
8.3 Chinese Version



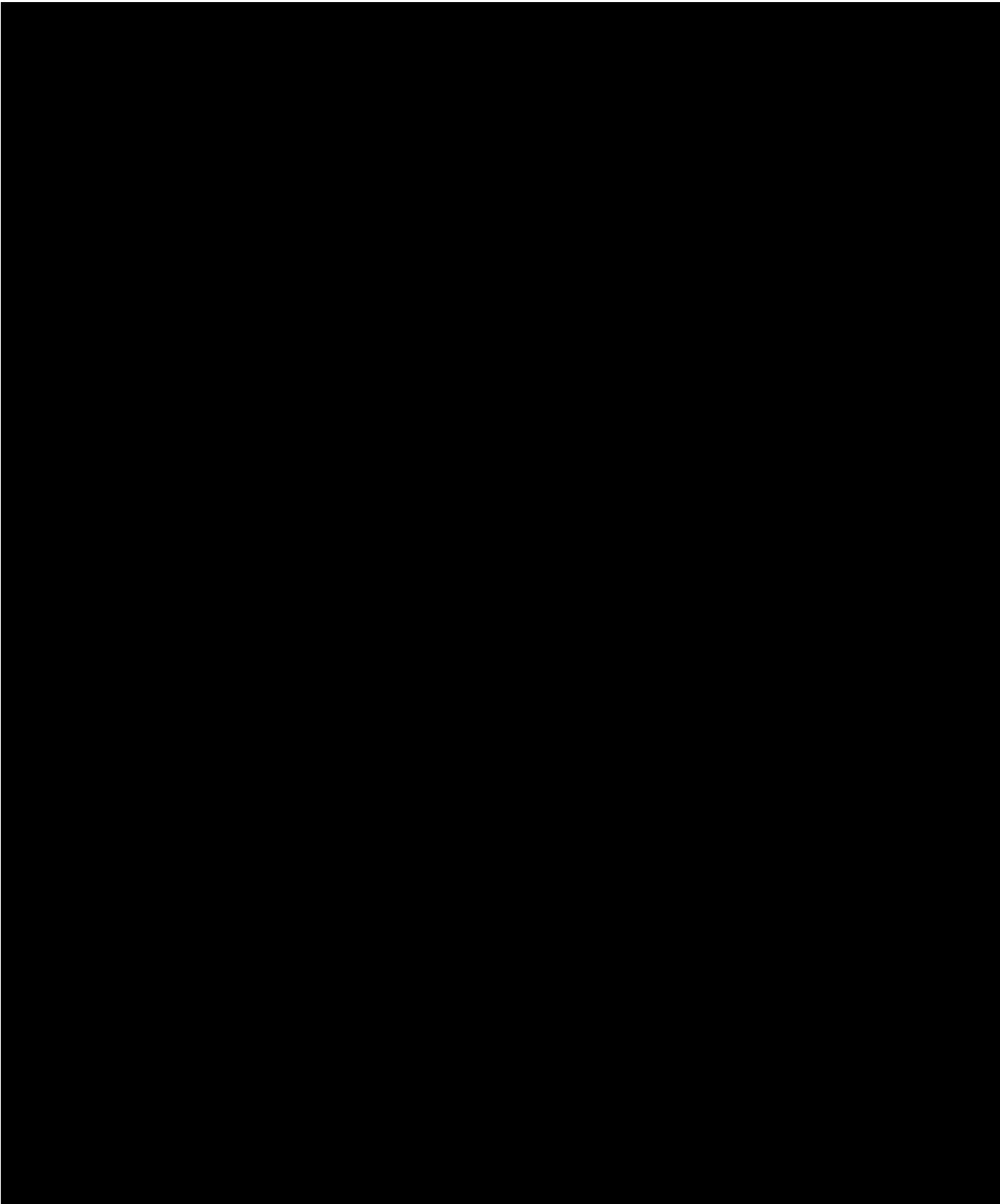


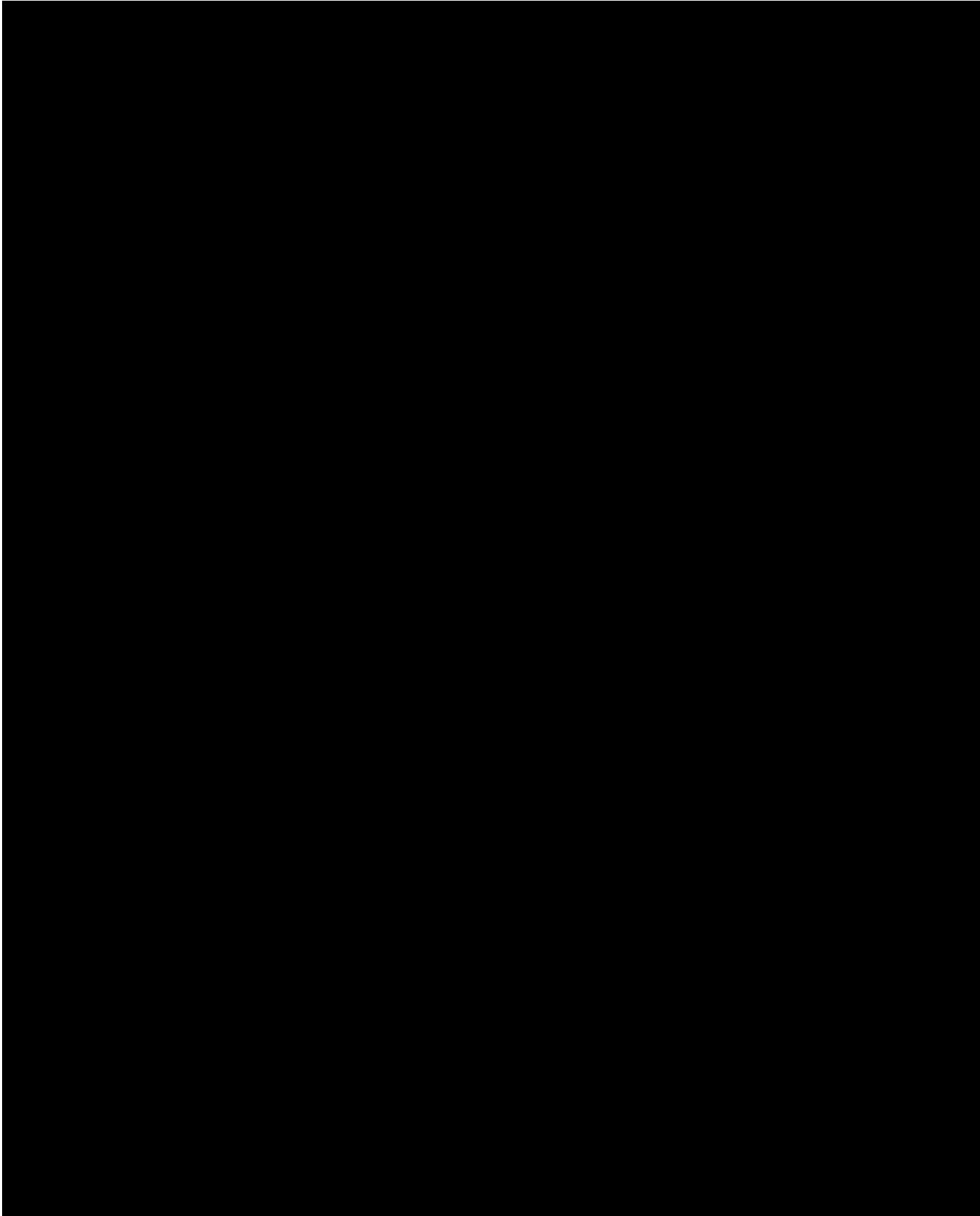


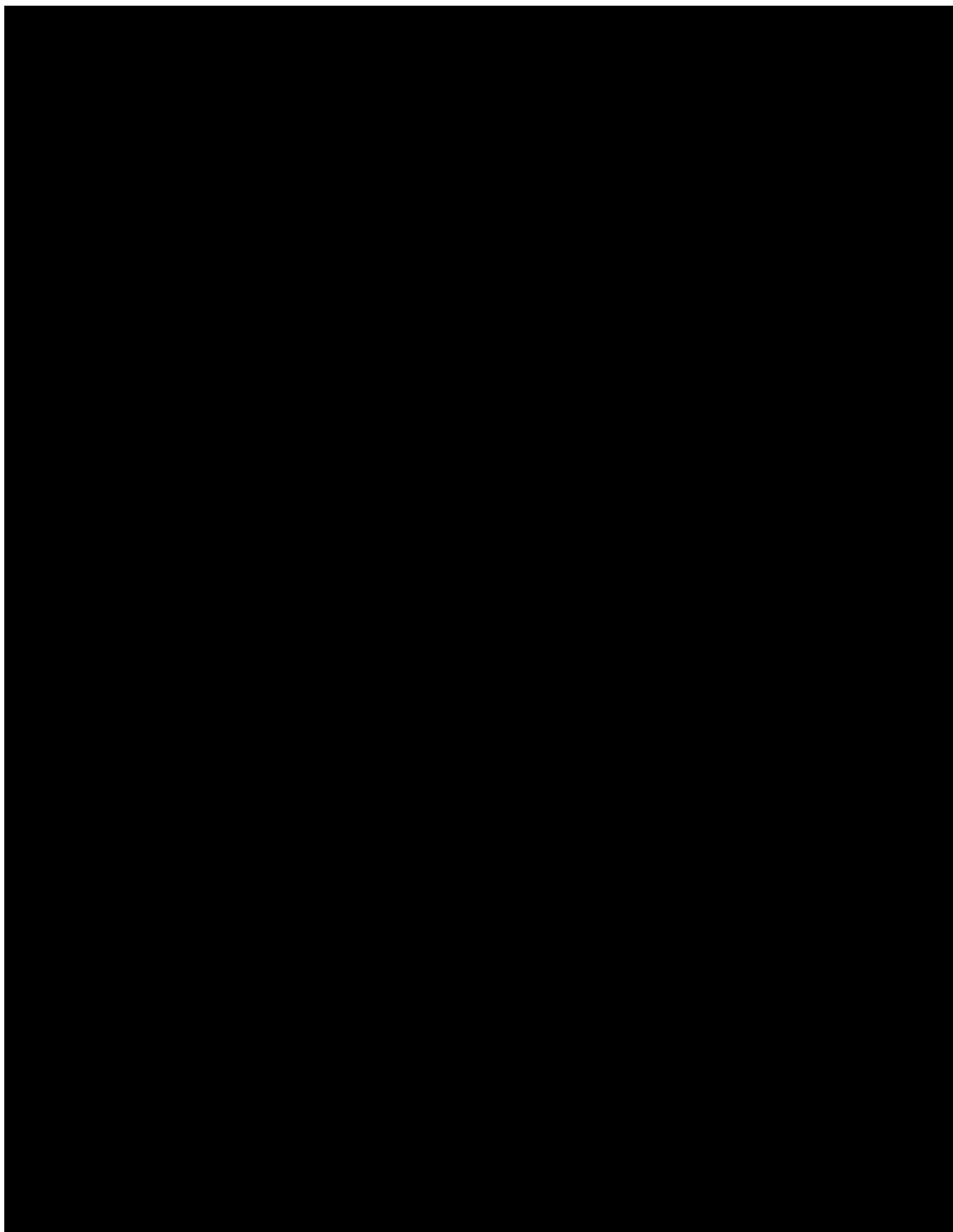


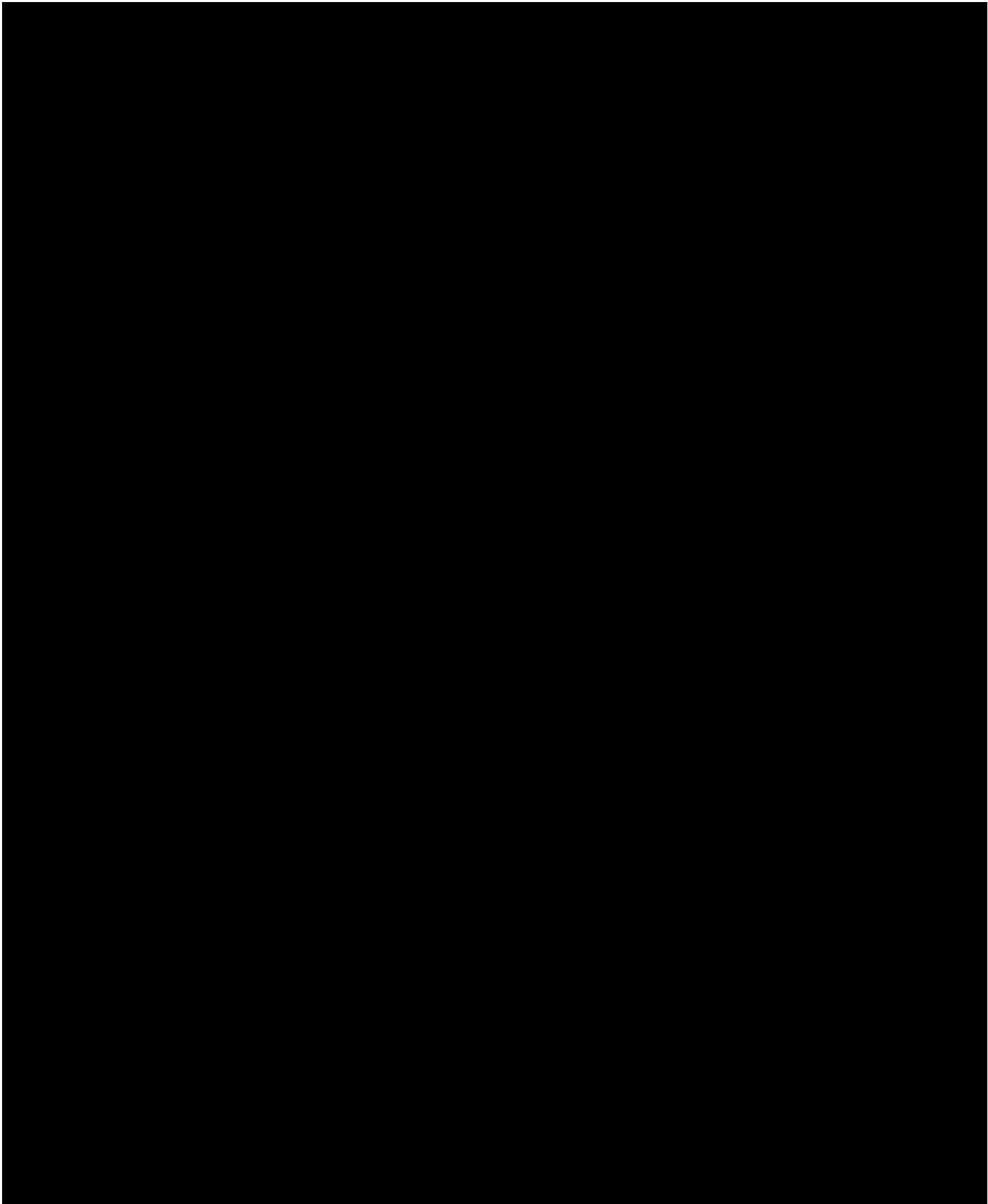


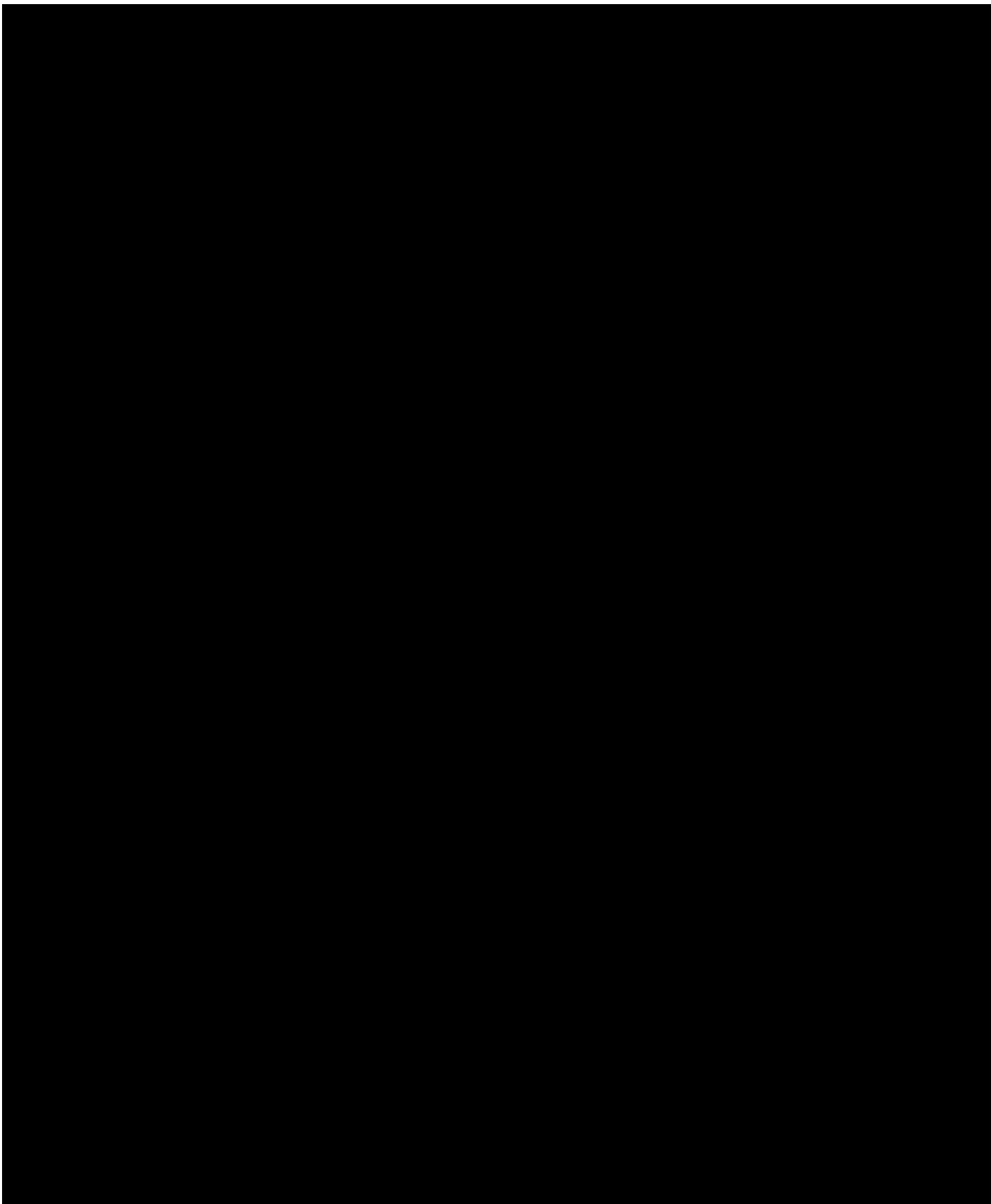
8.4 Arabic Version

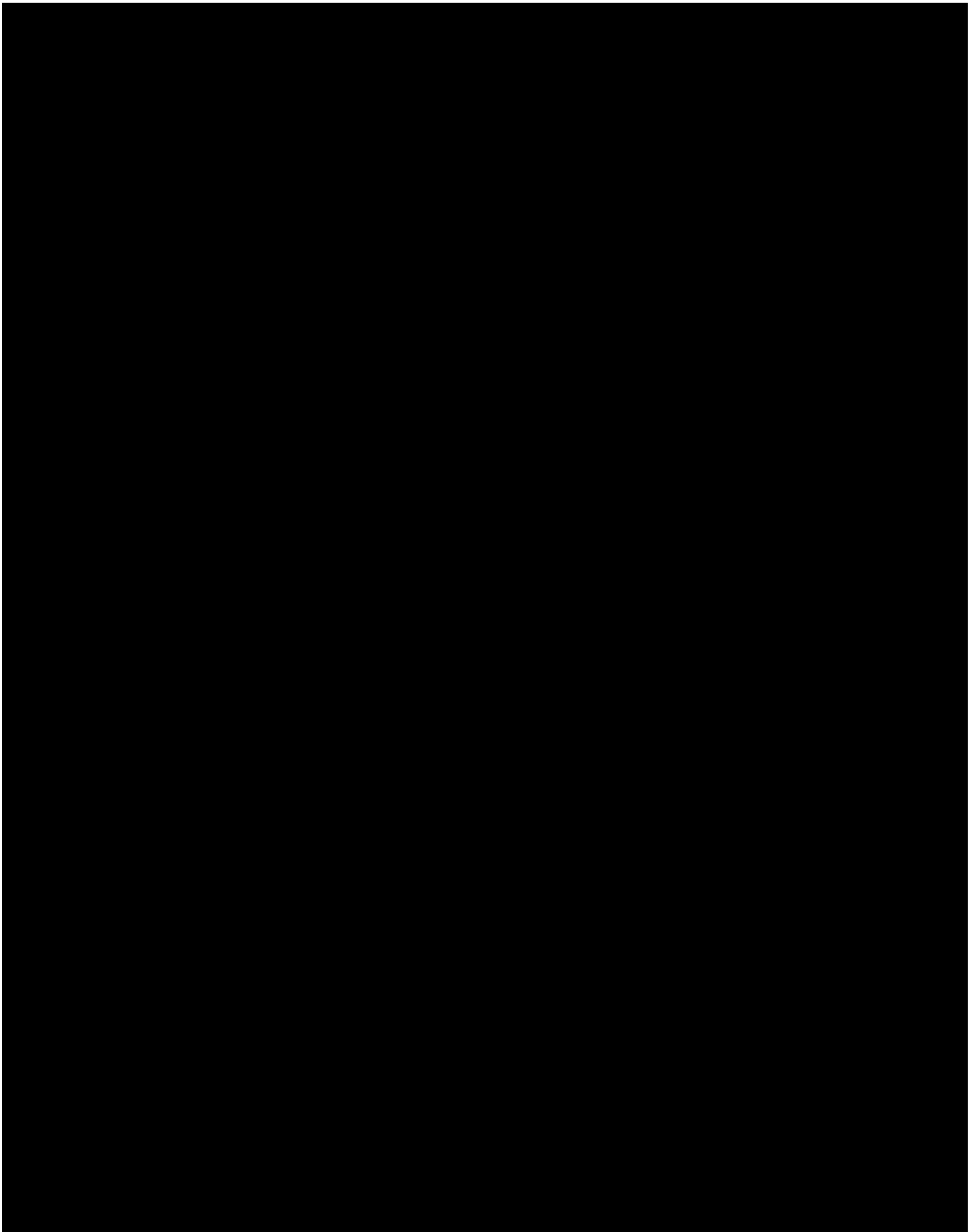


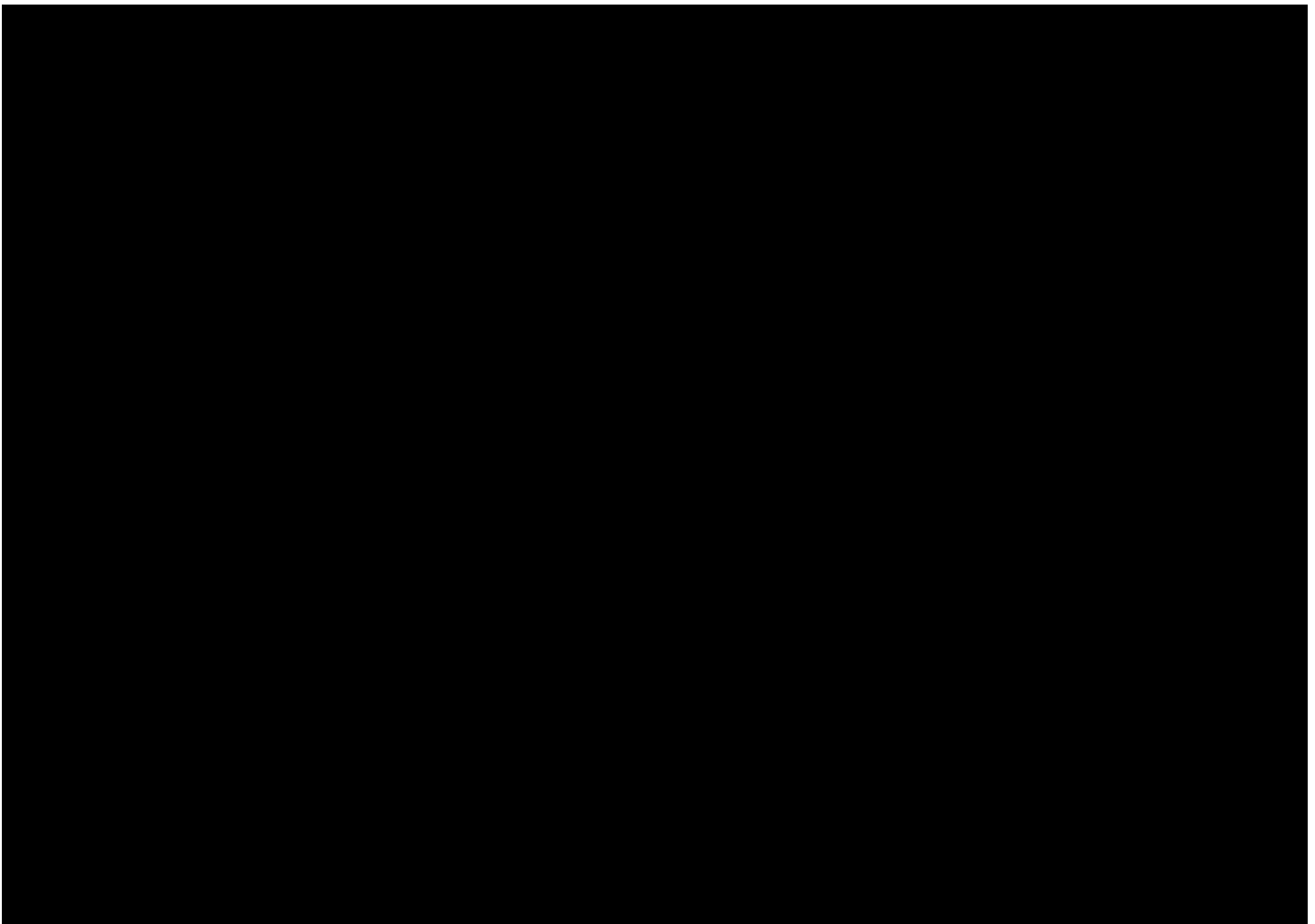




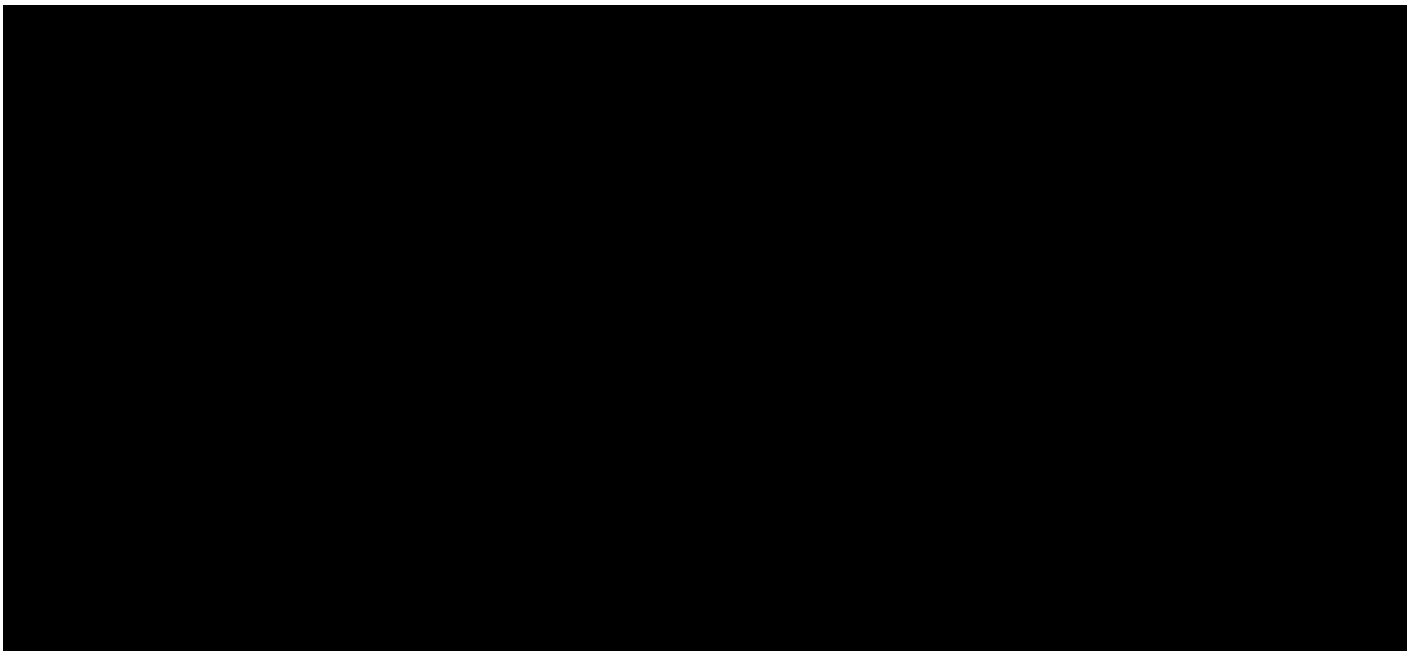


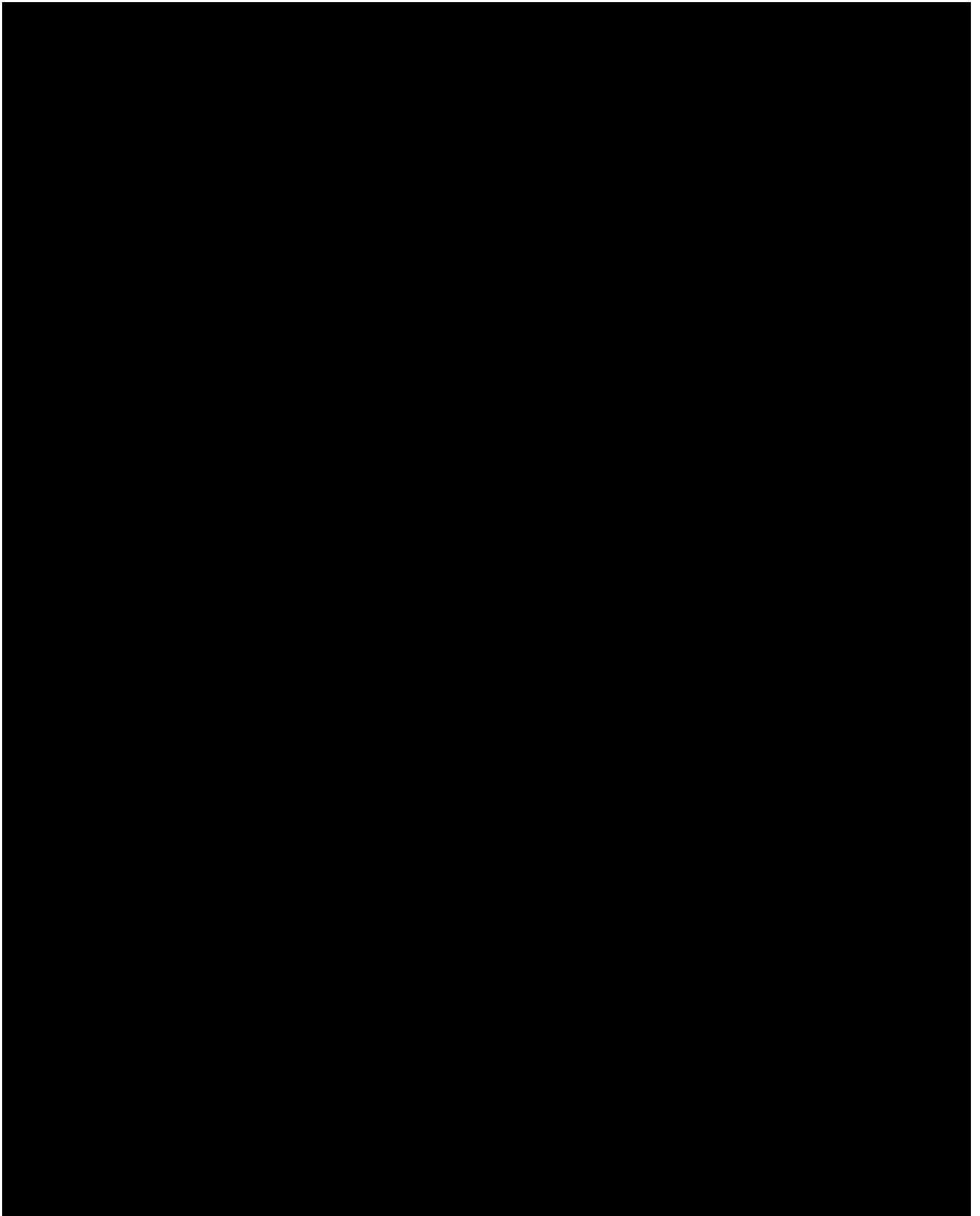


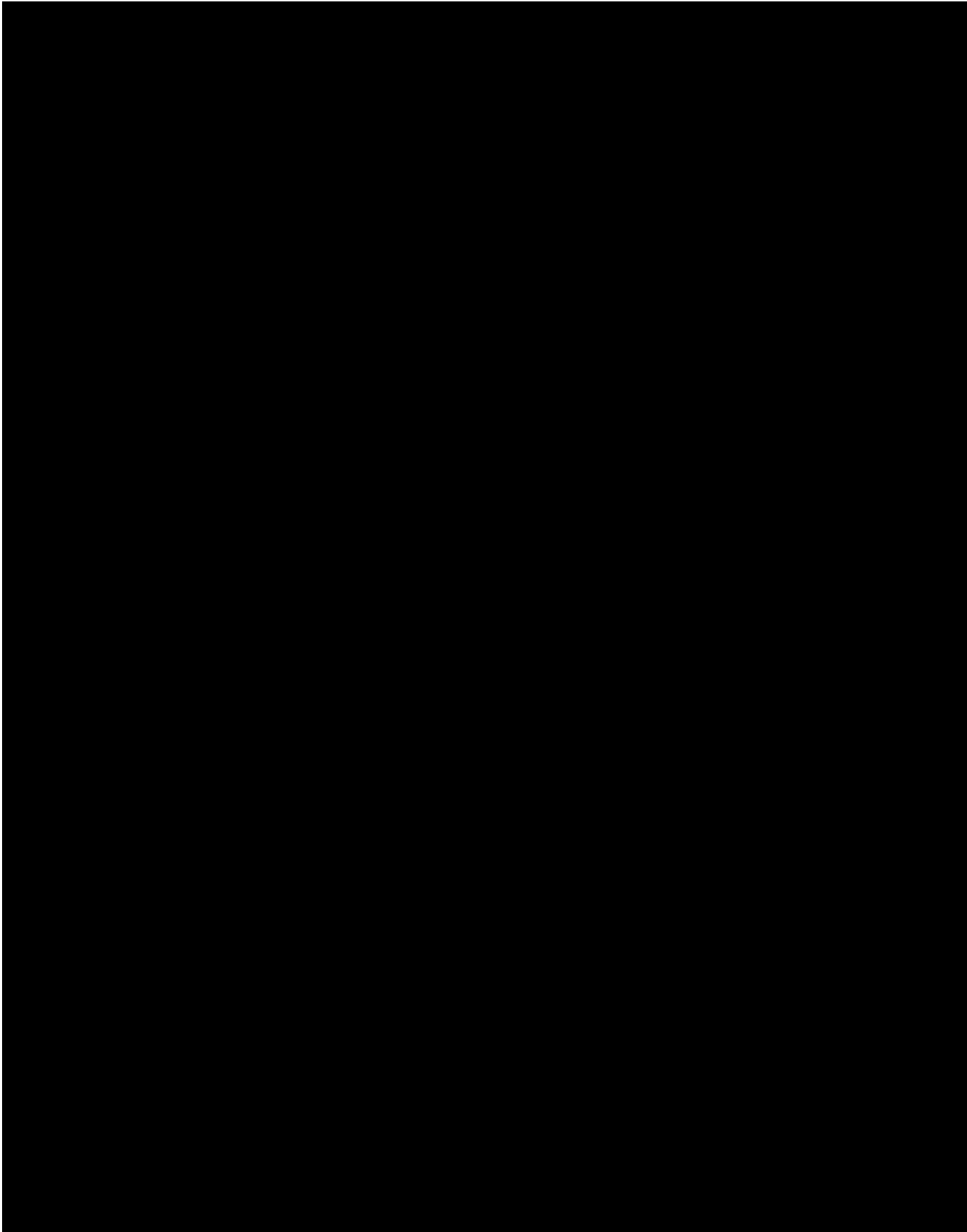


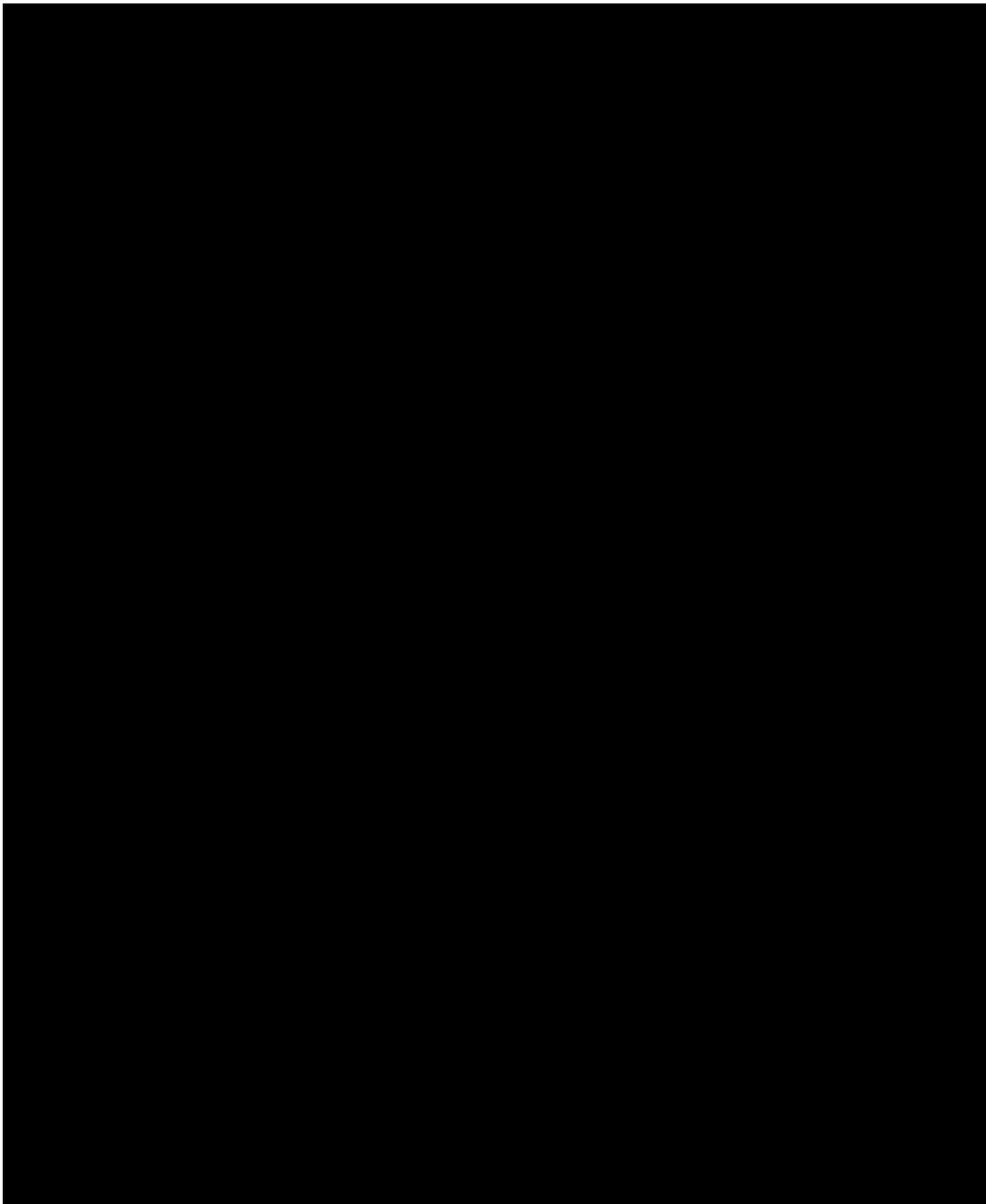


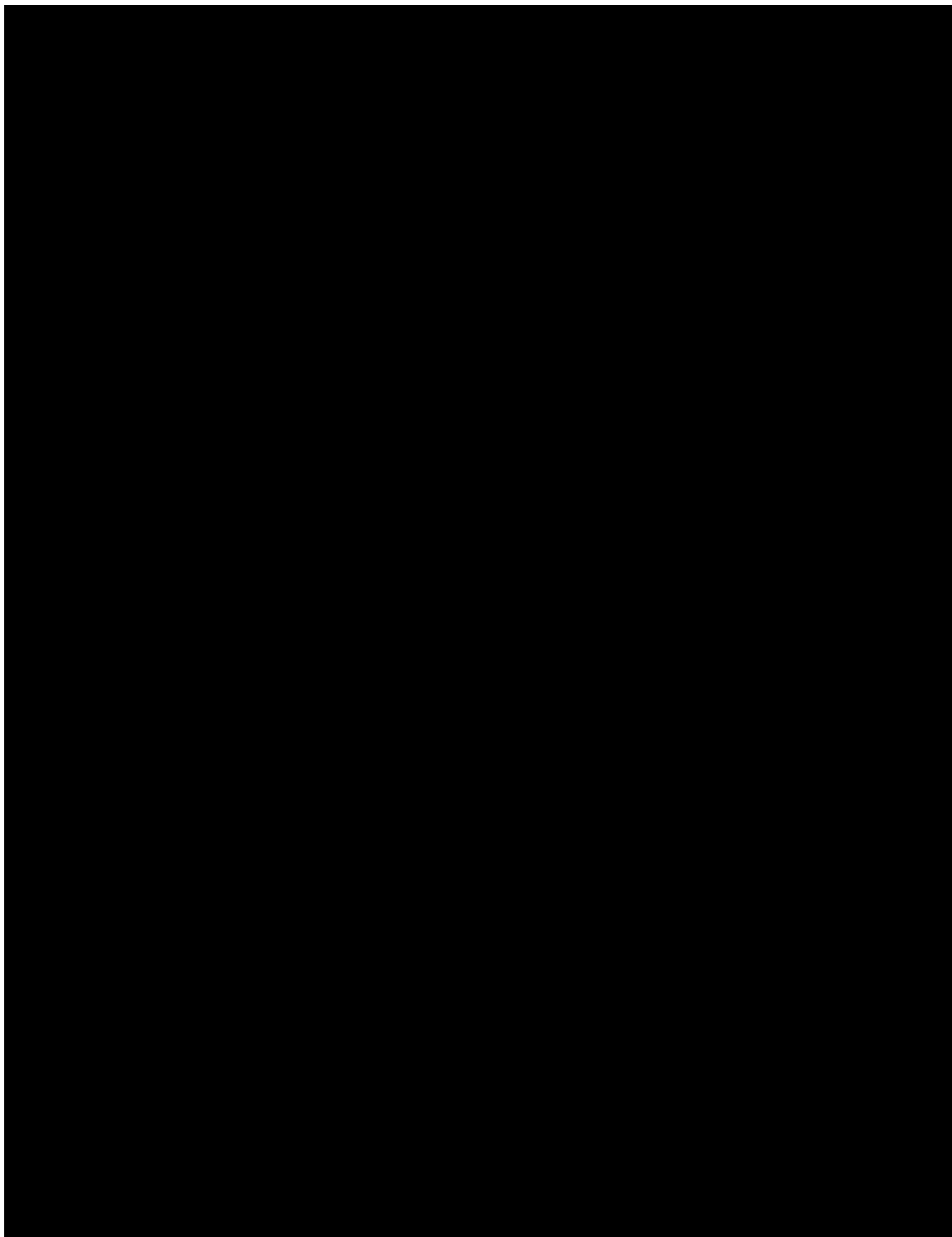
8.5 French Version

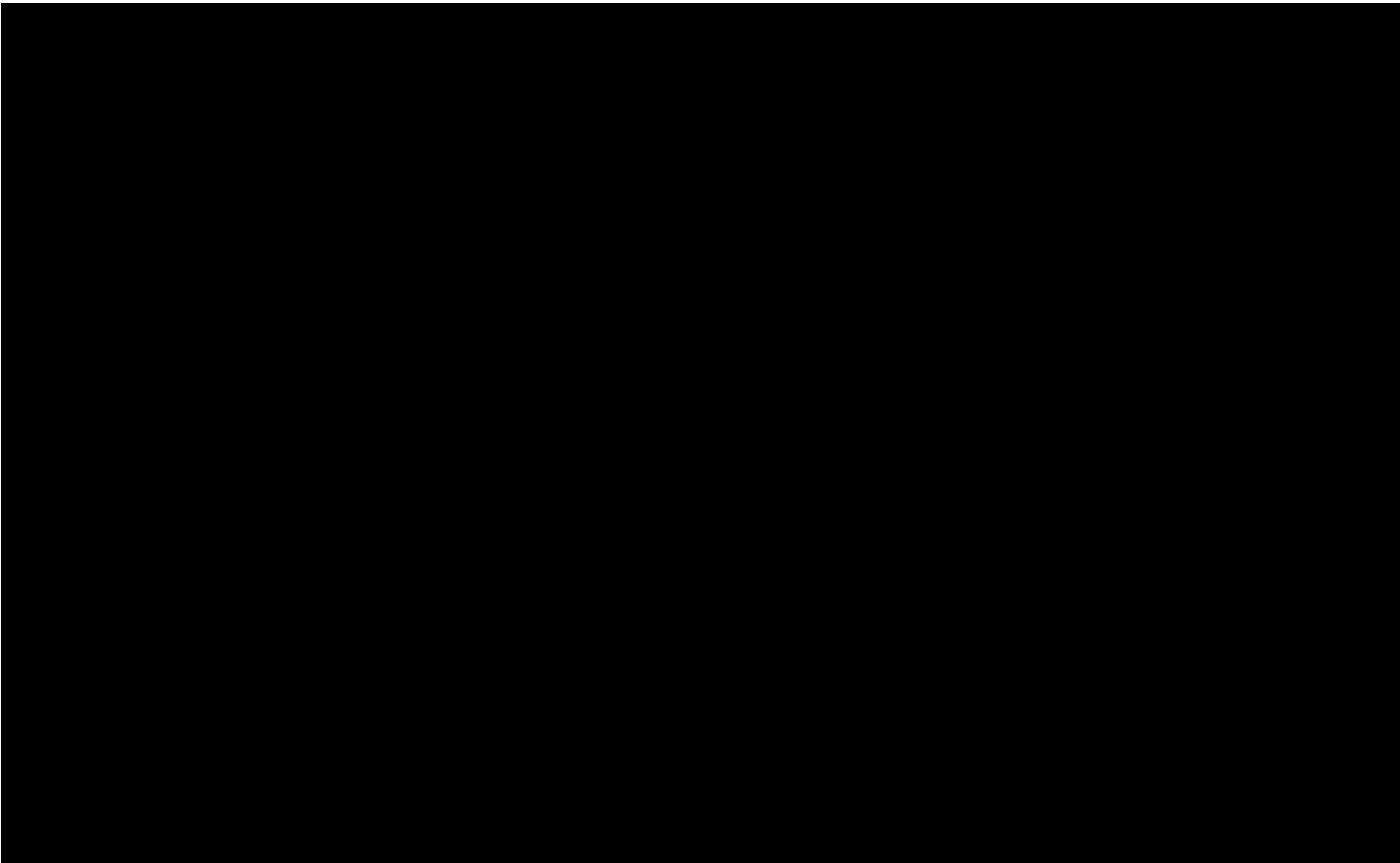




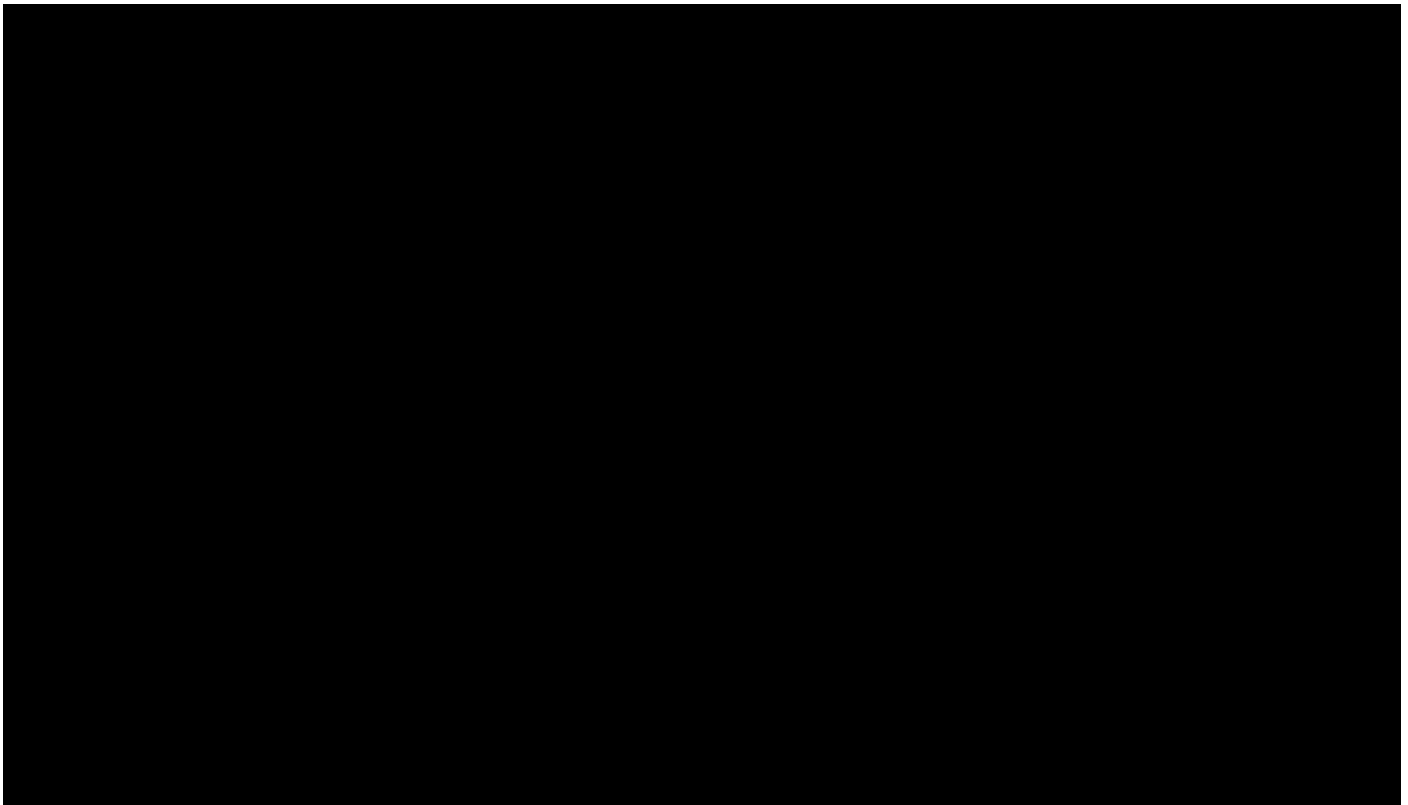


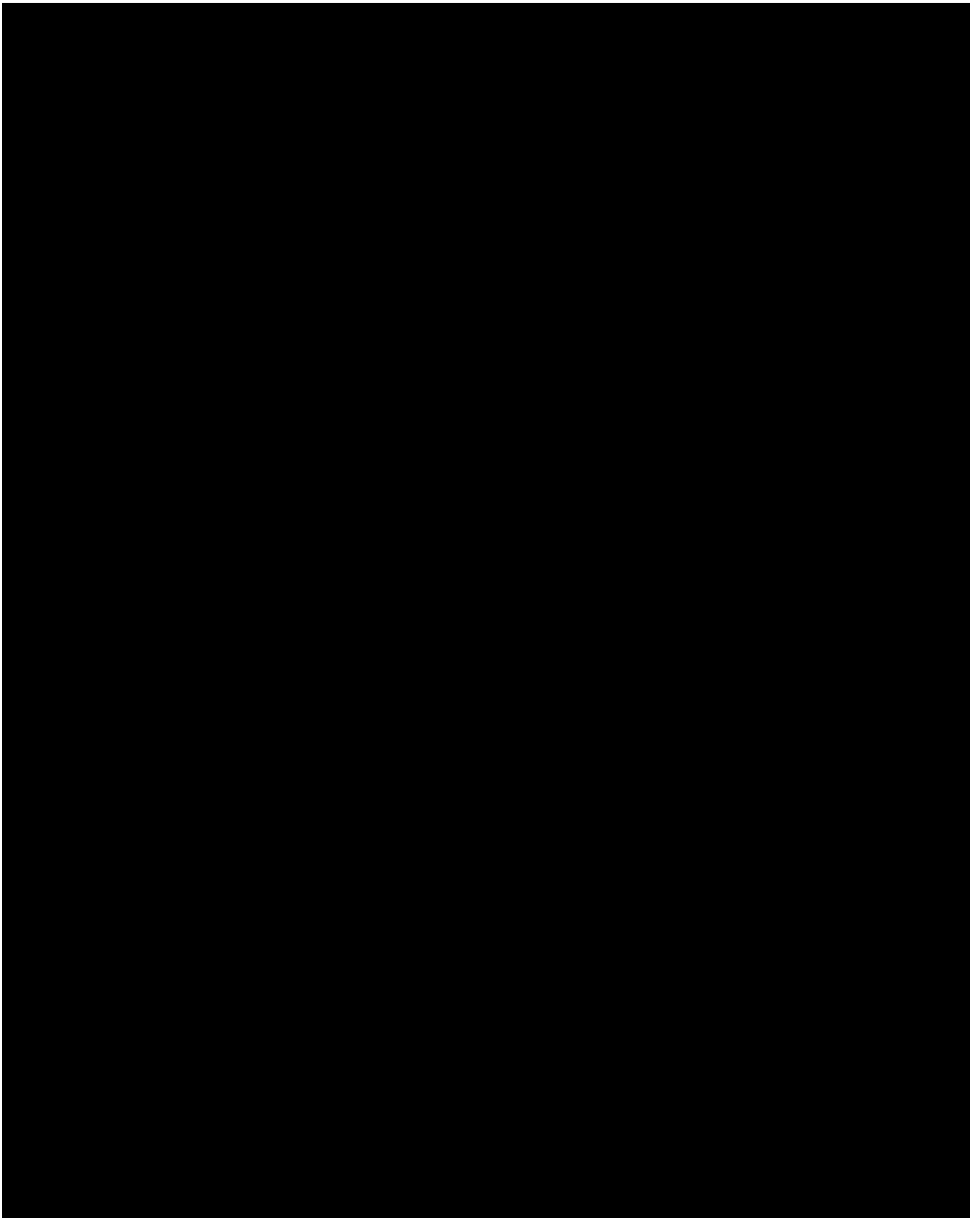


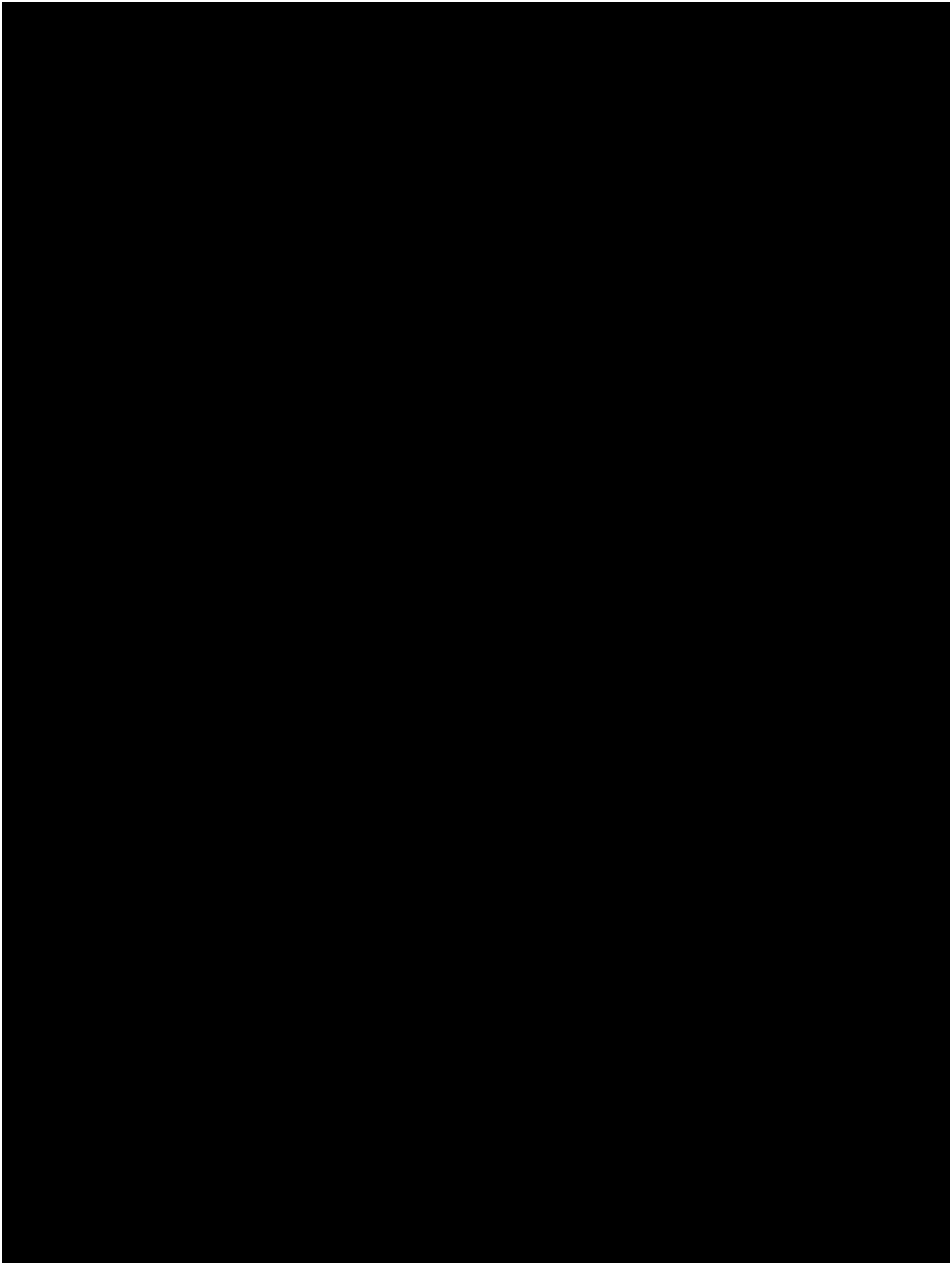


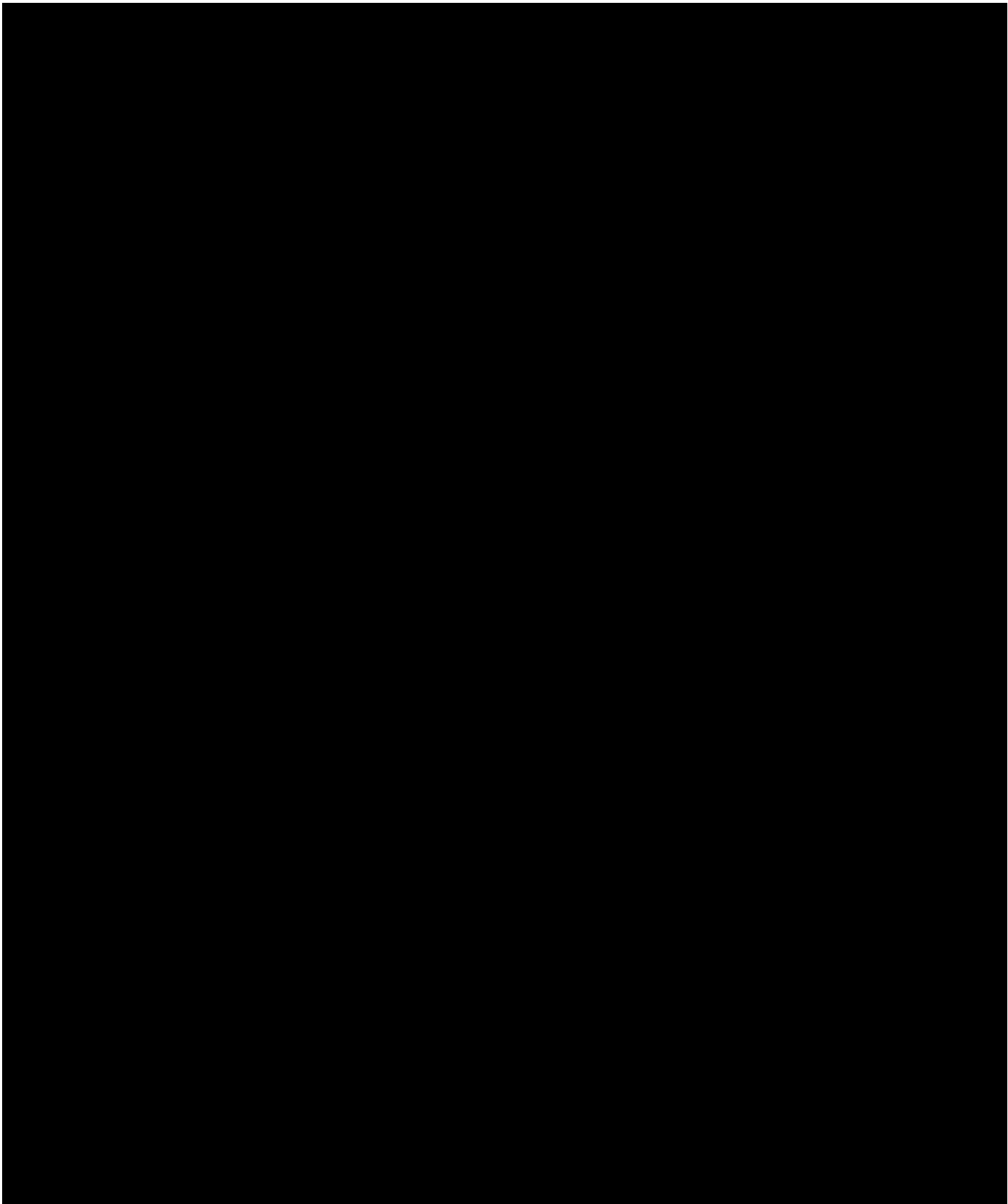


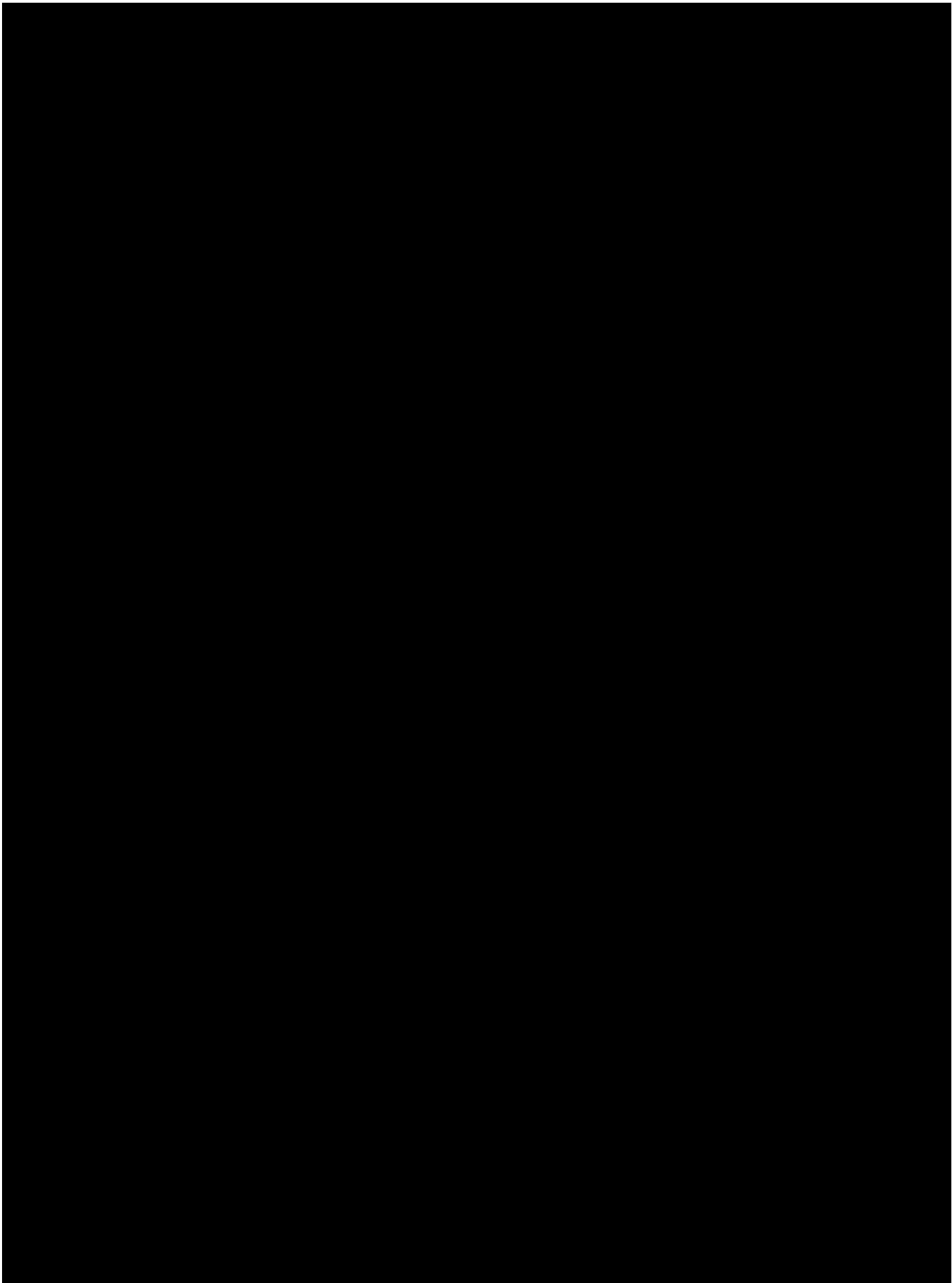
8.6 German Version

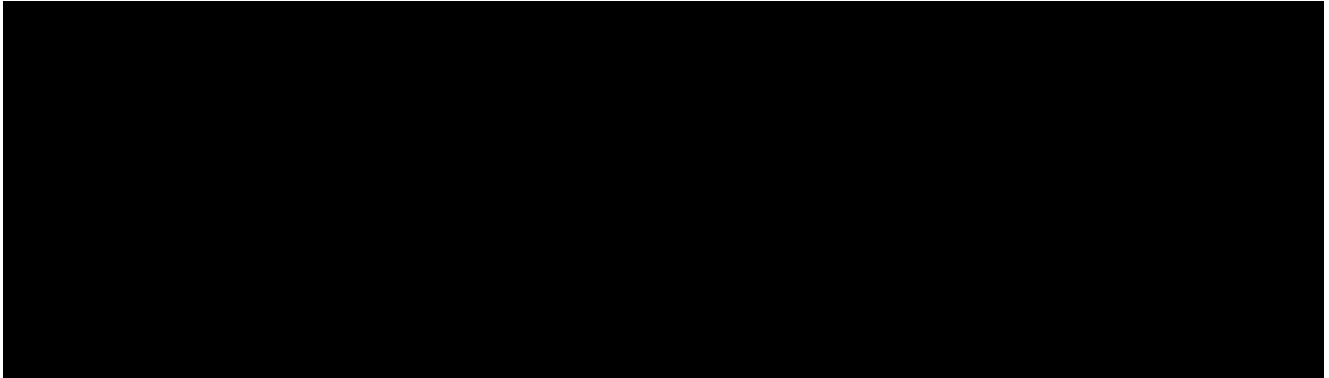




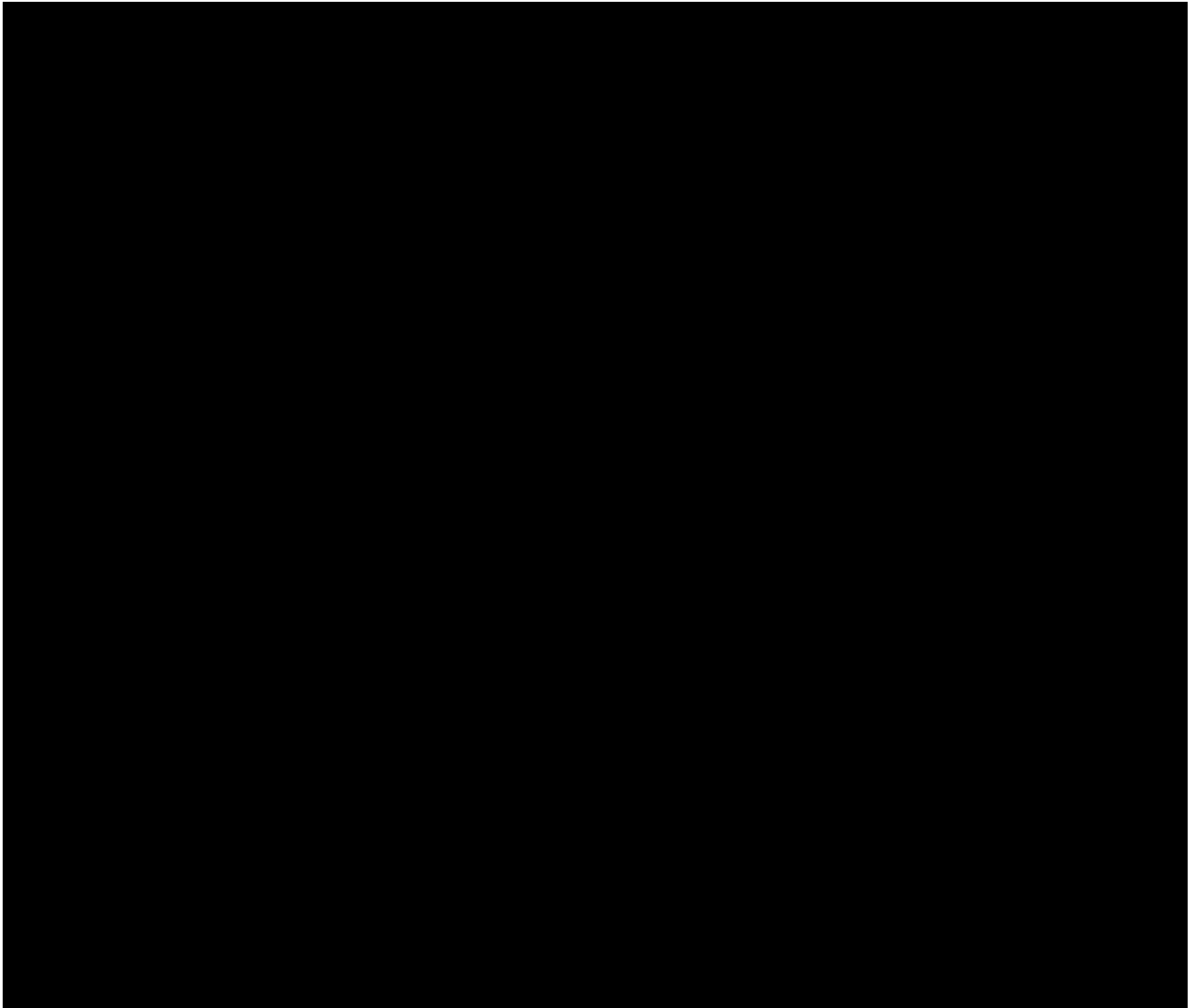


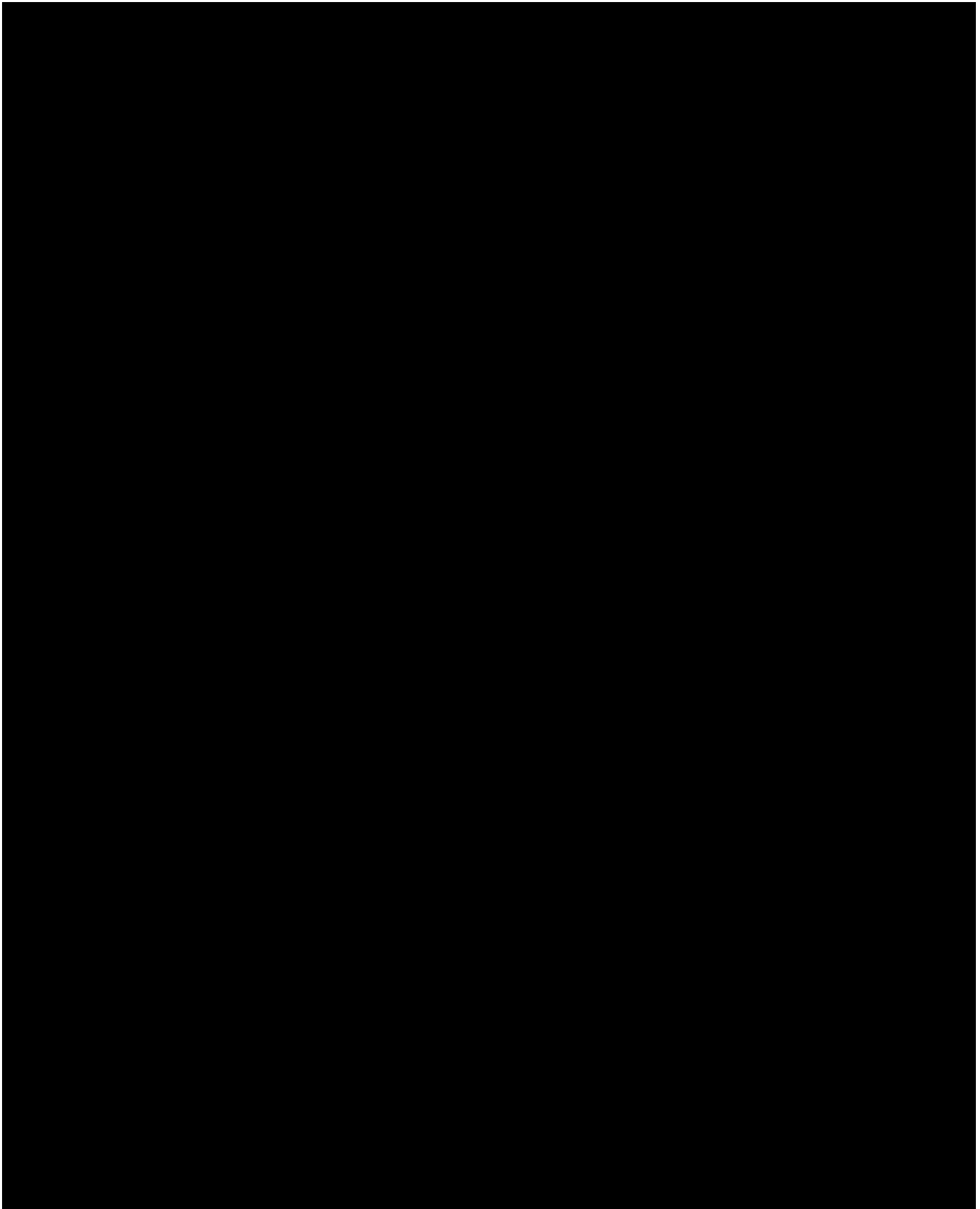


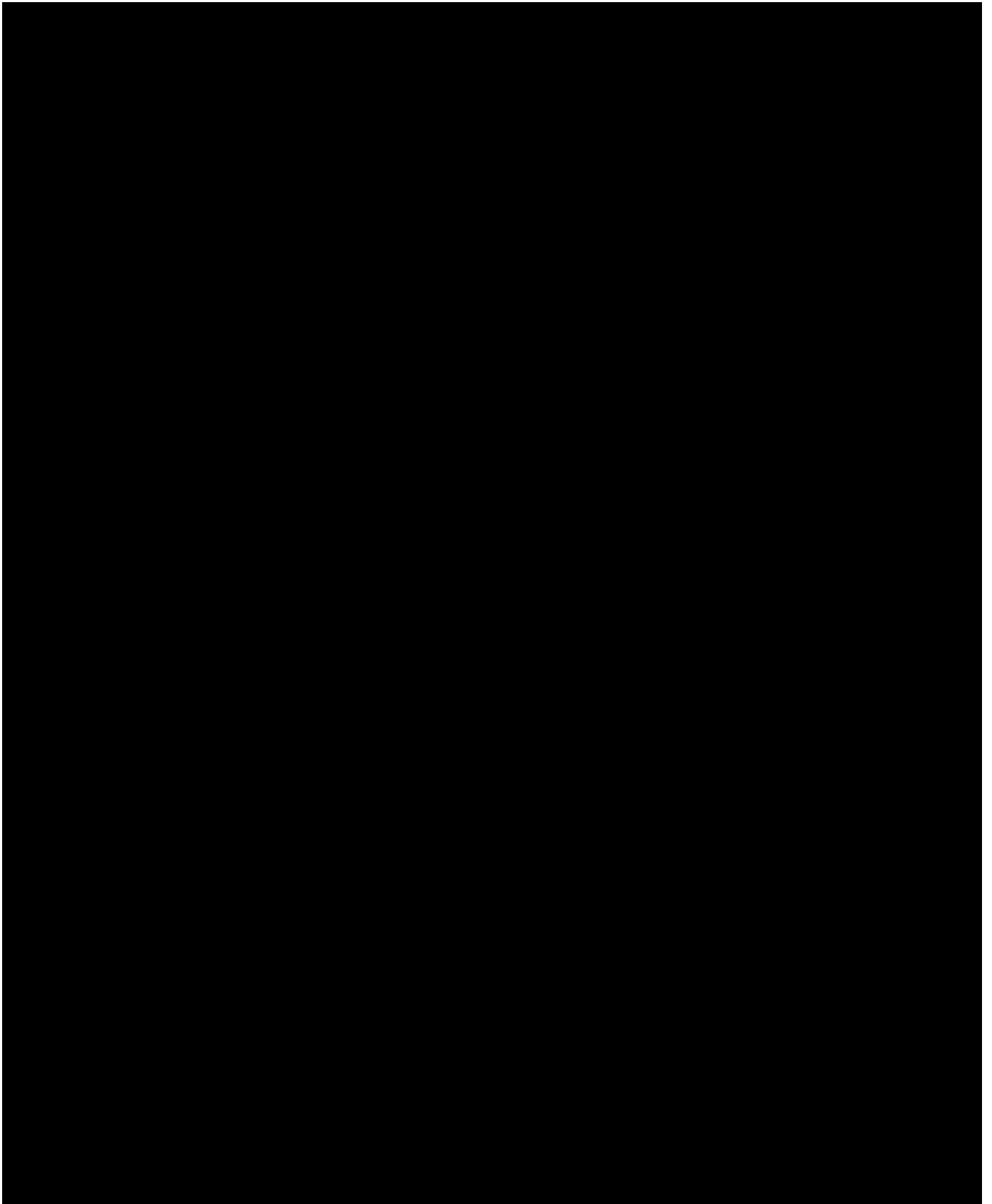


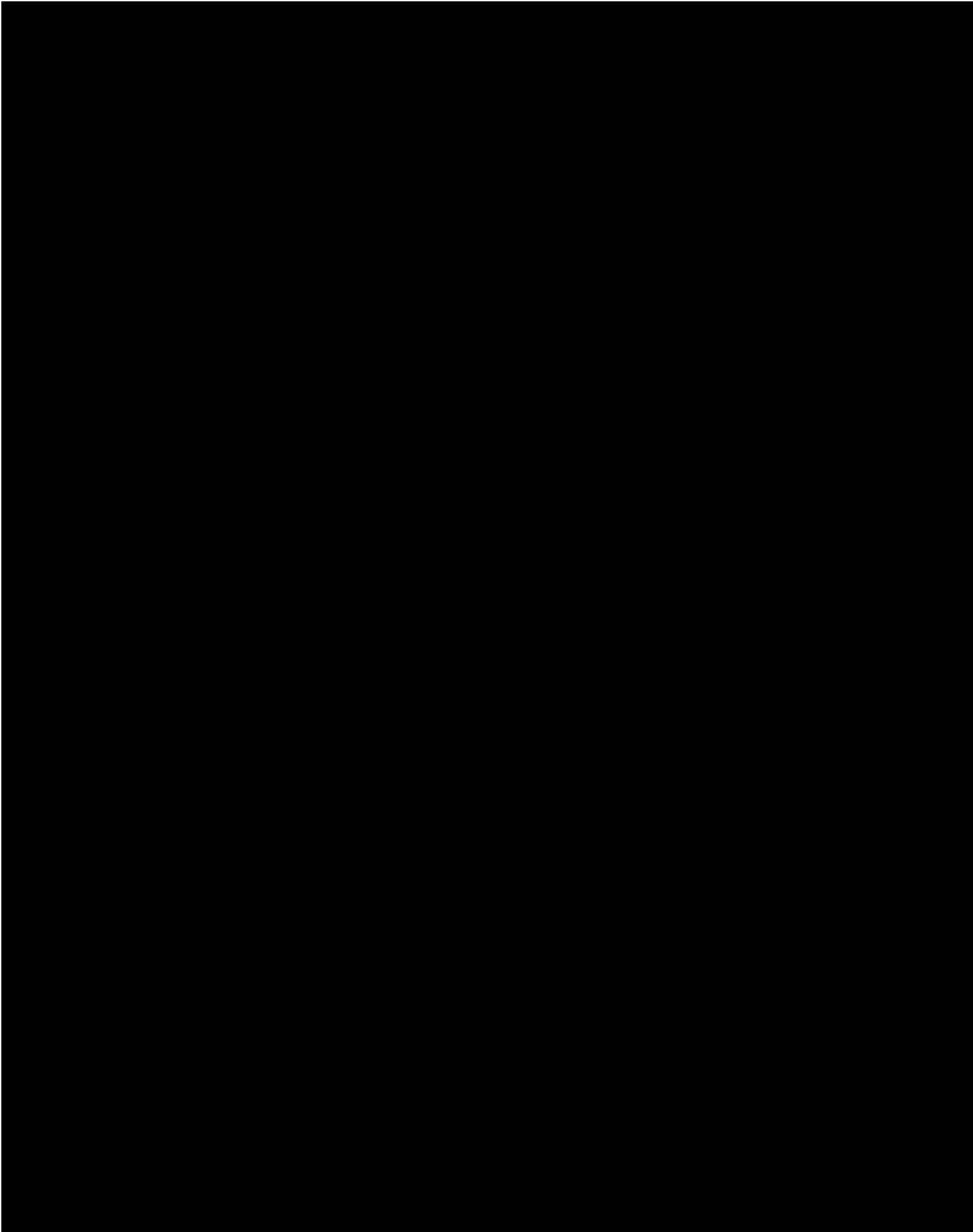


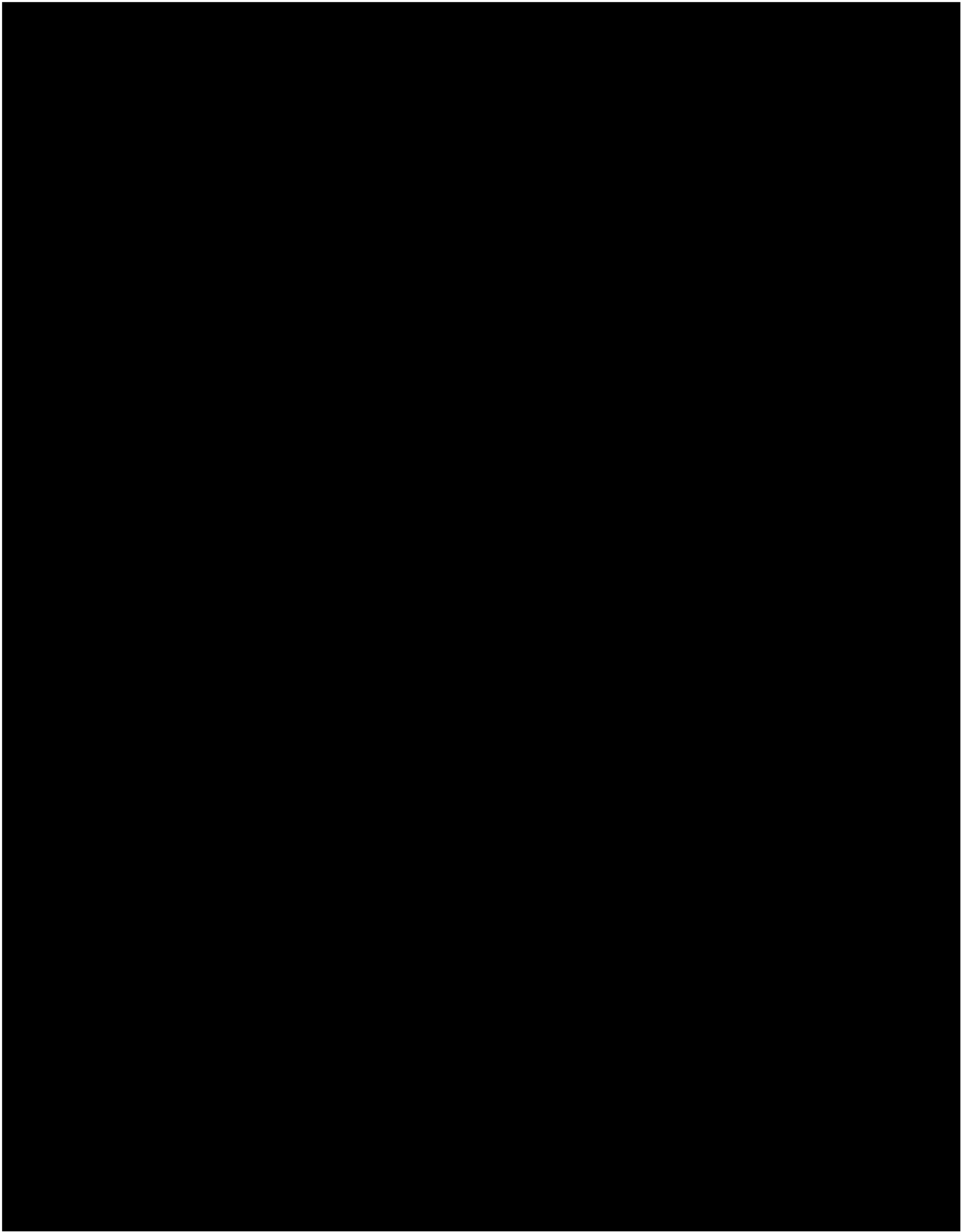
8.7 Russian Version

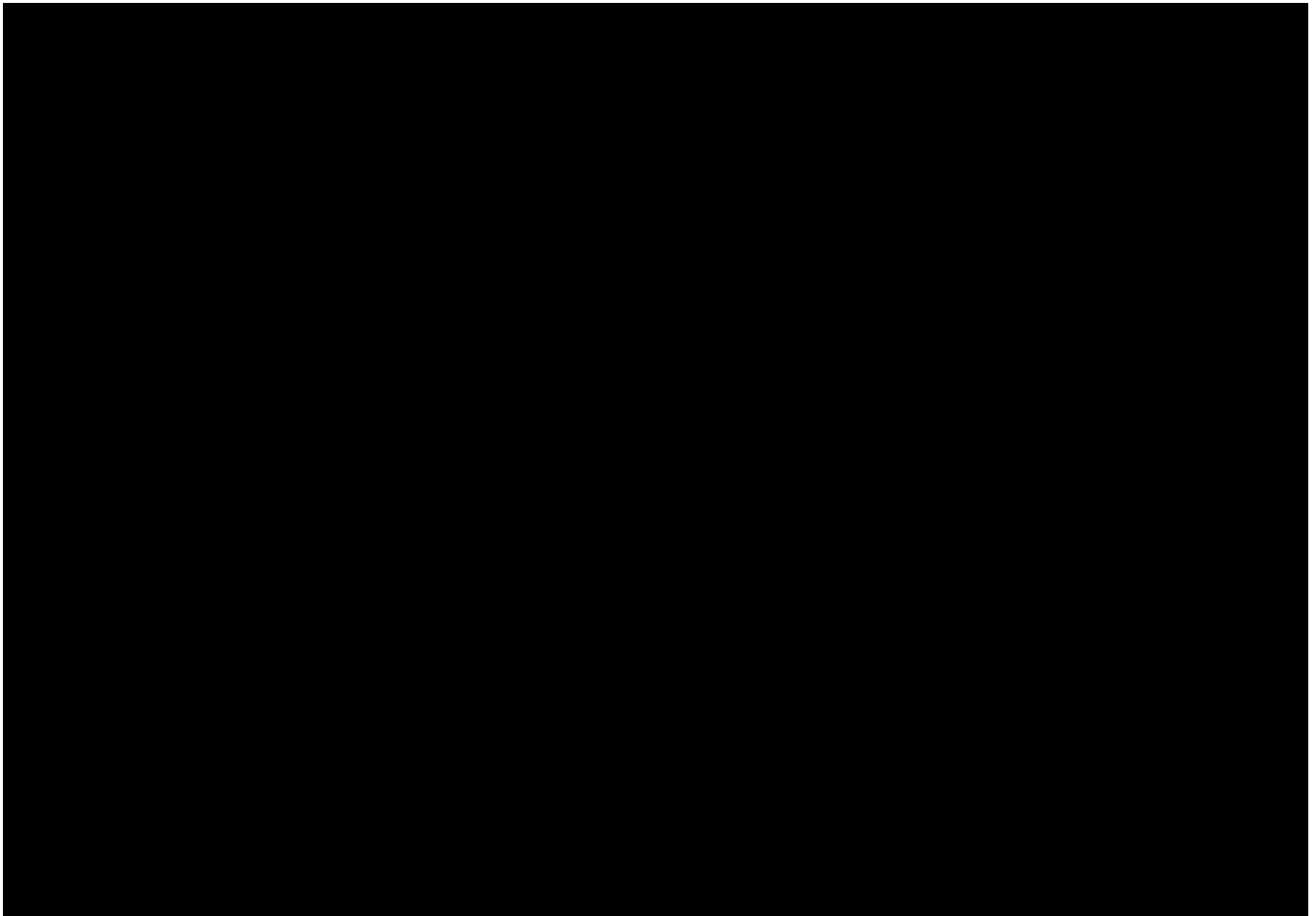




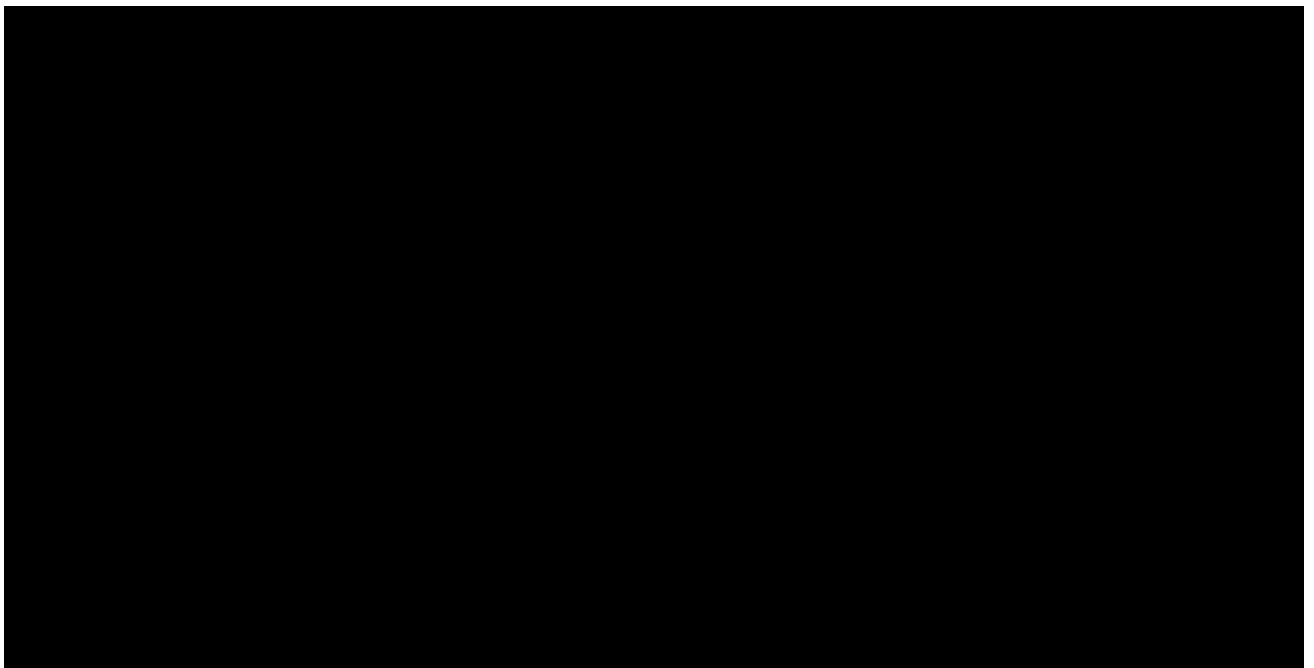


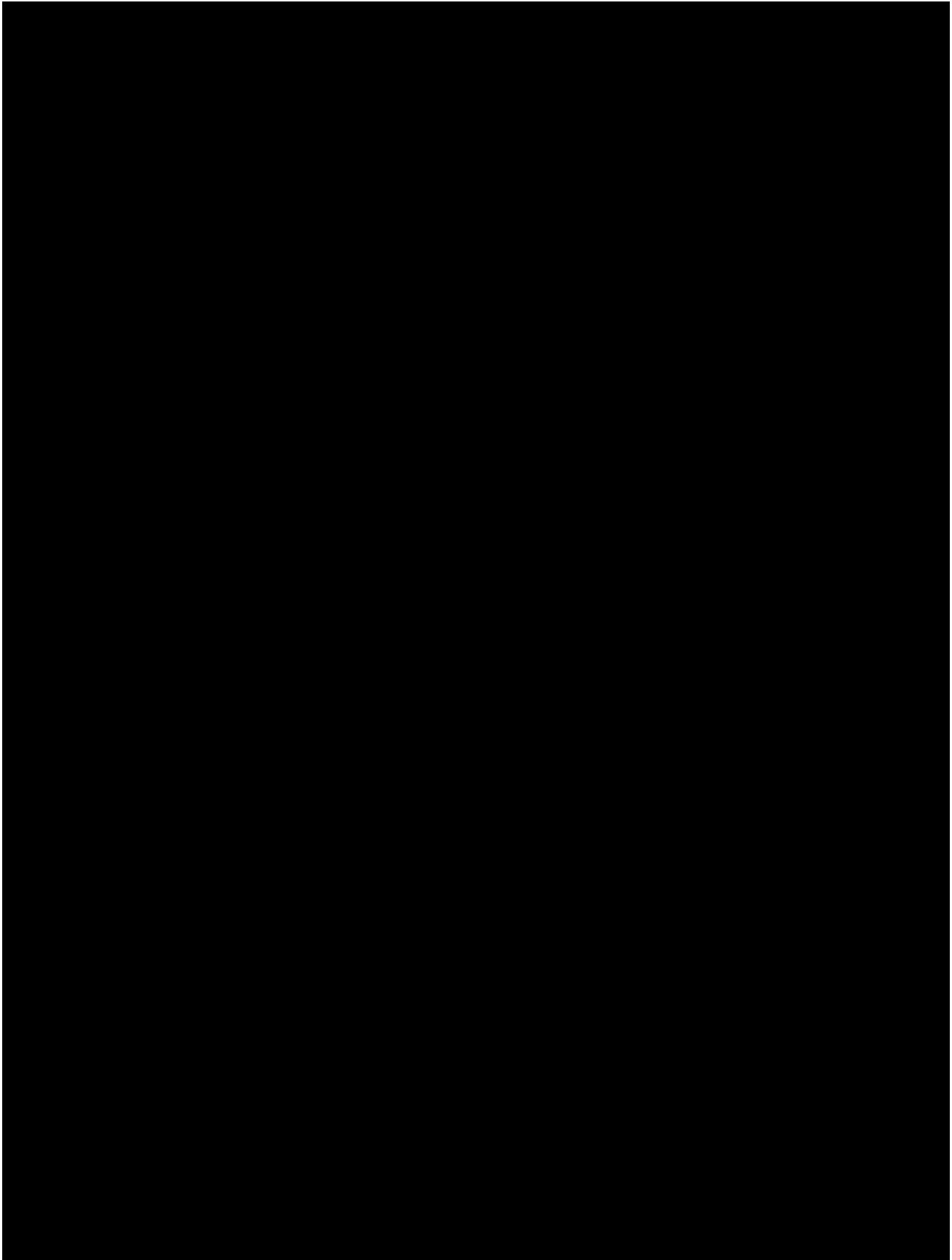


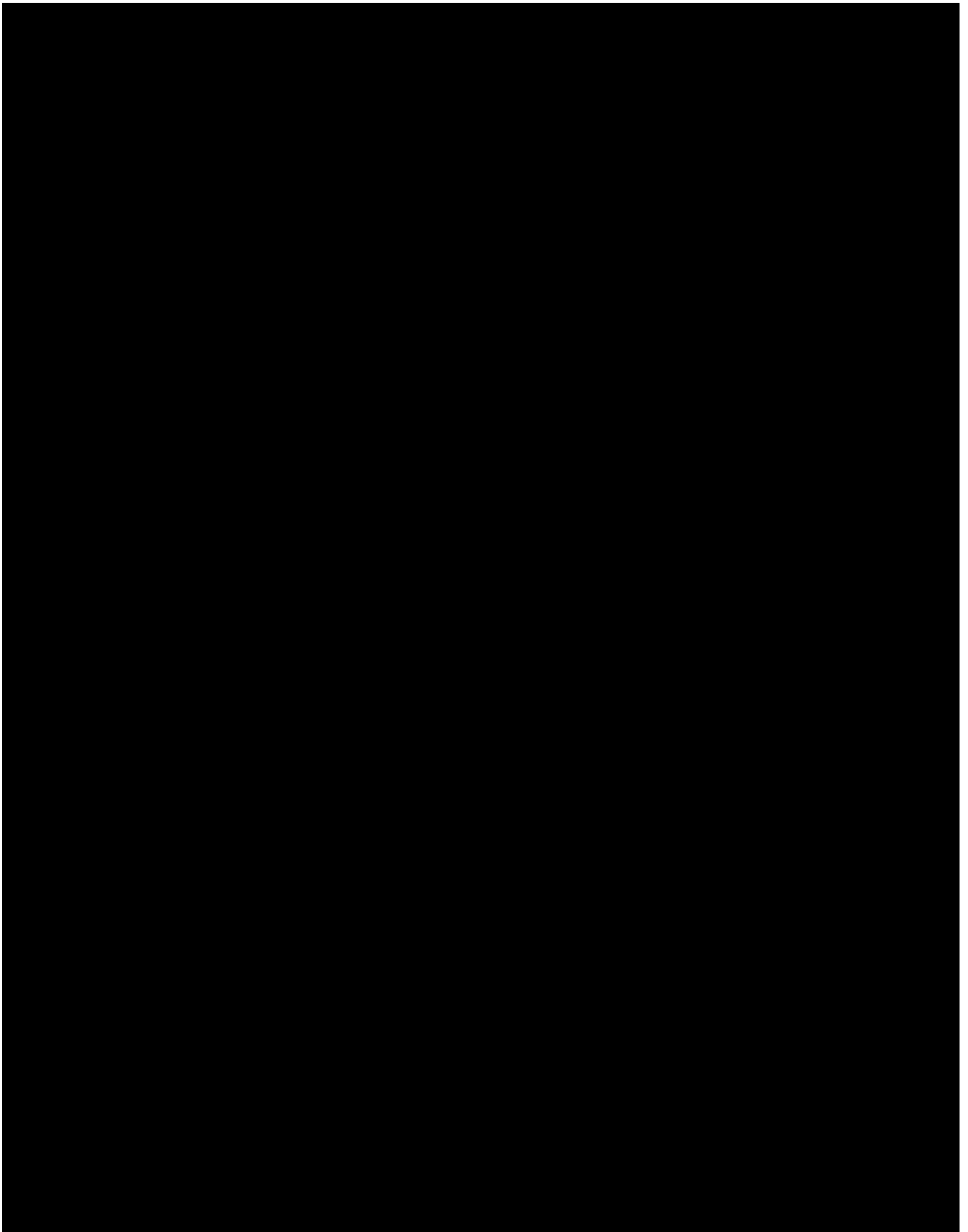


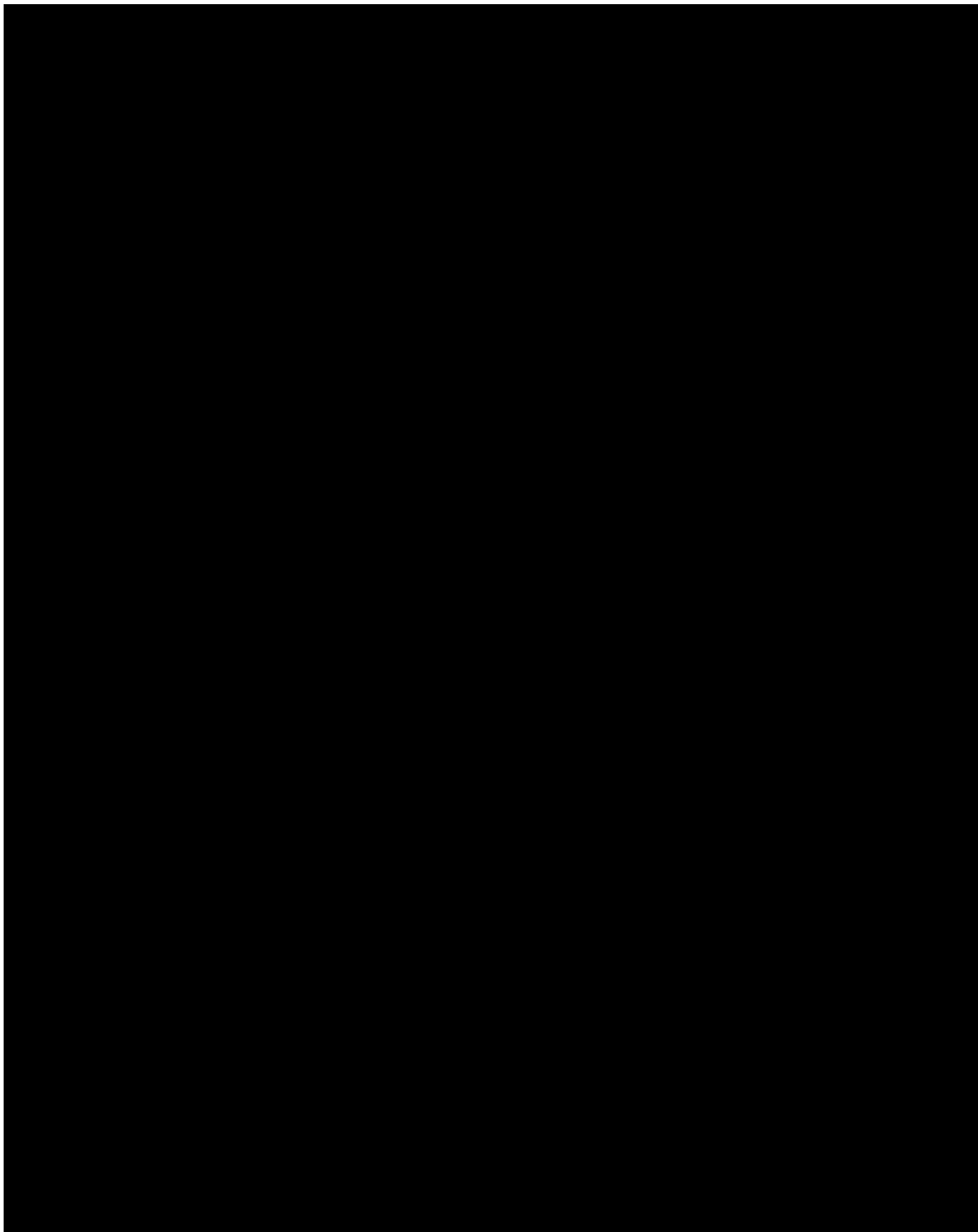


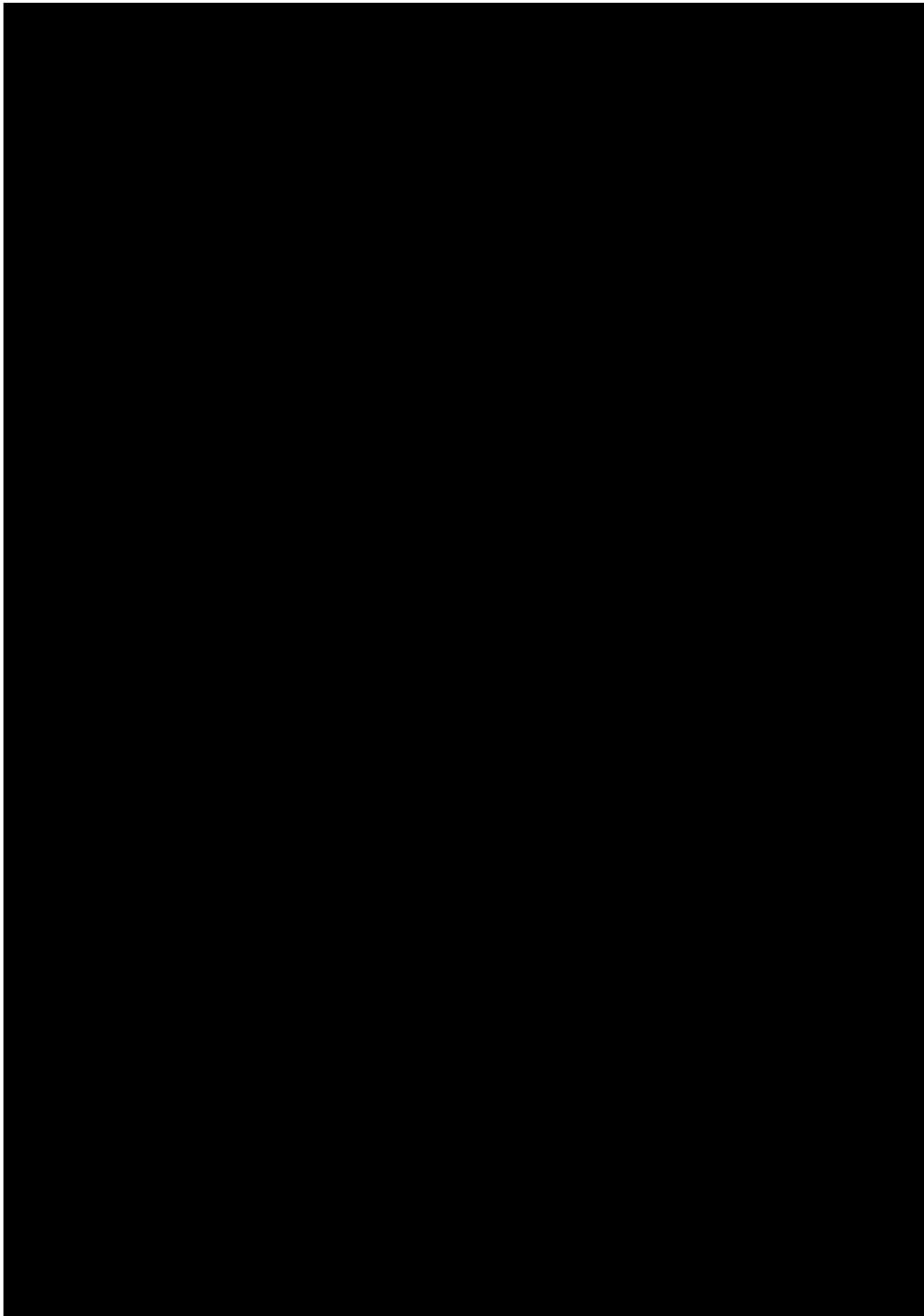
8.8 Spanish Version

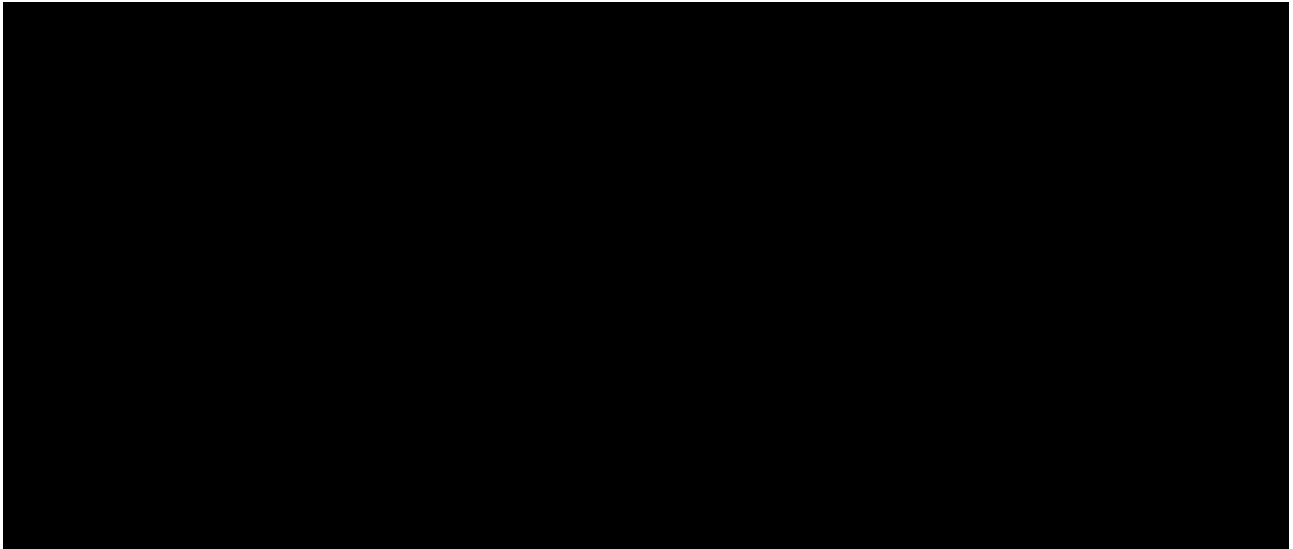




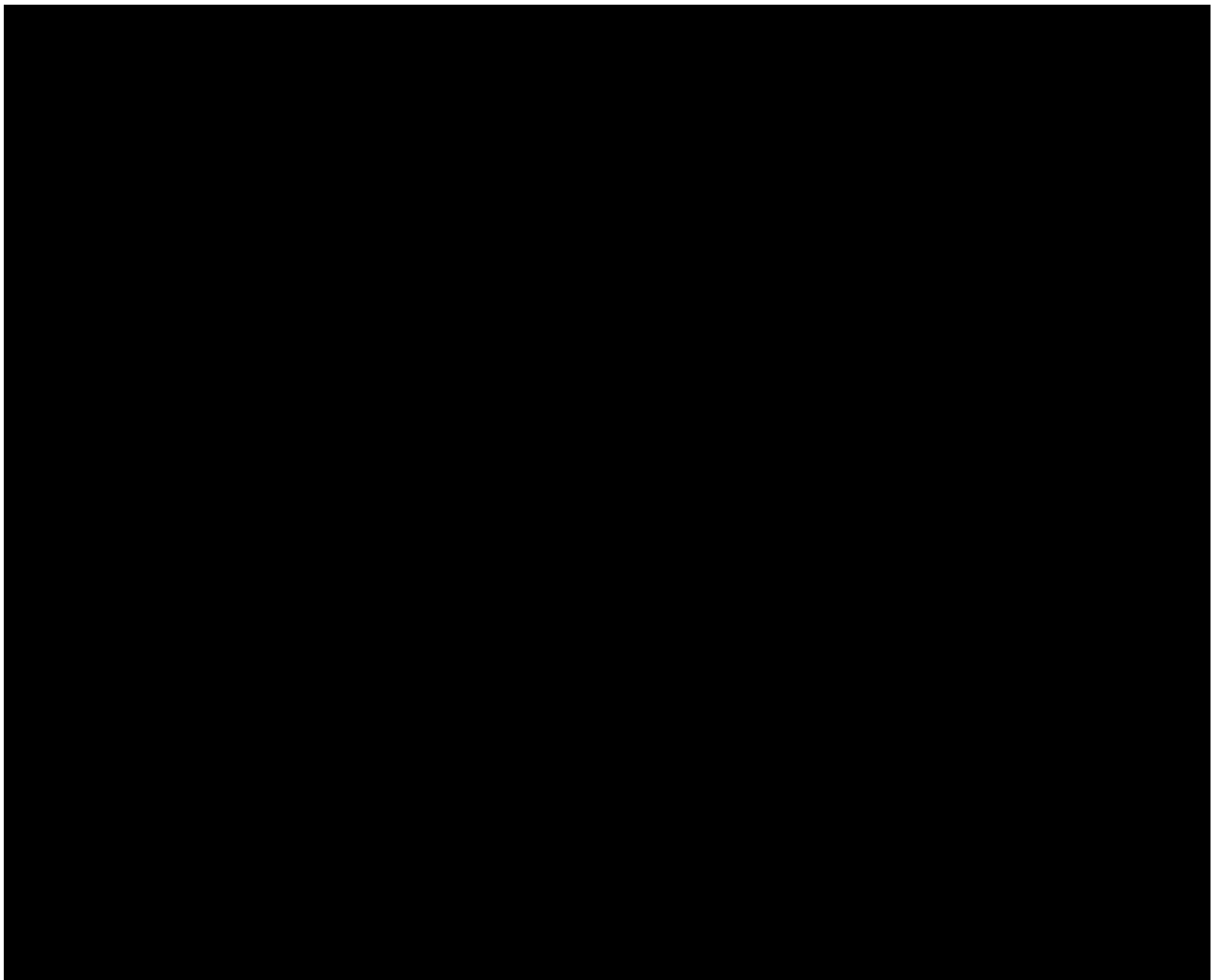


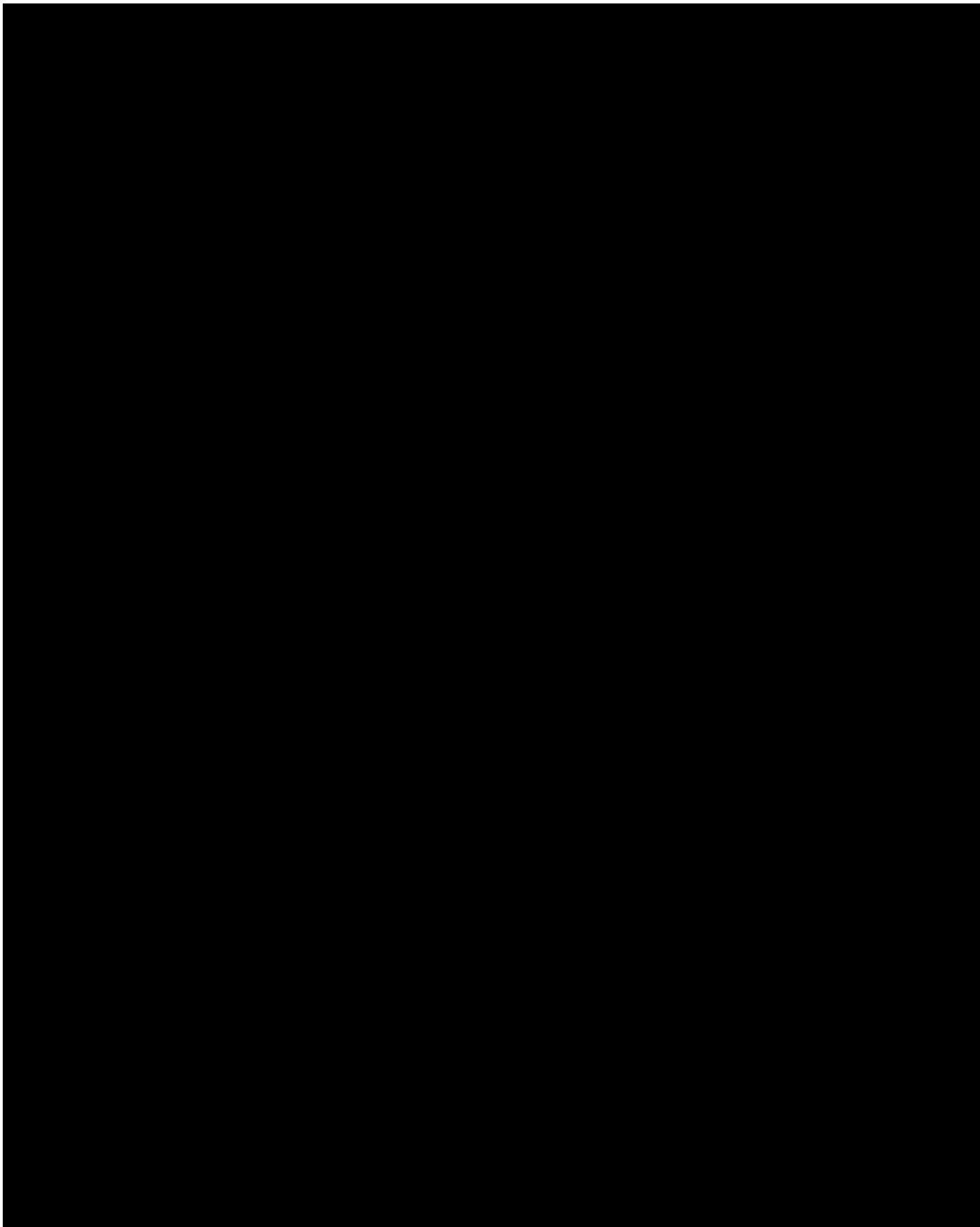


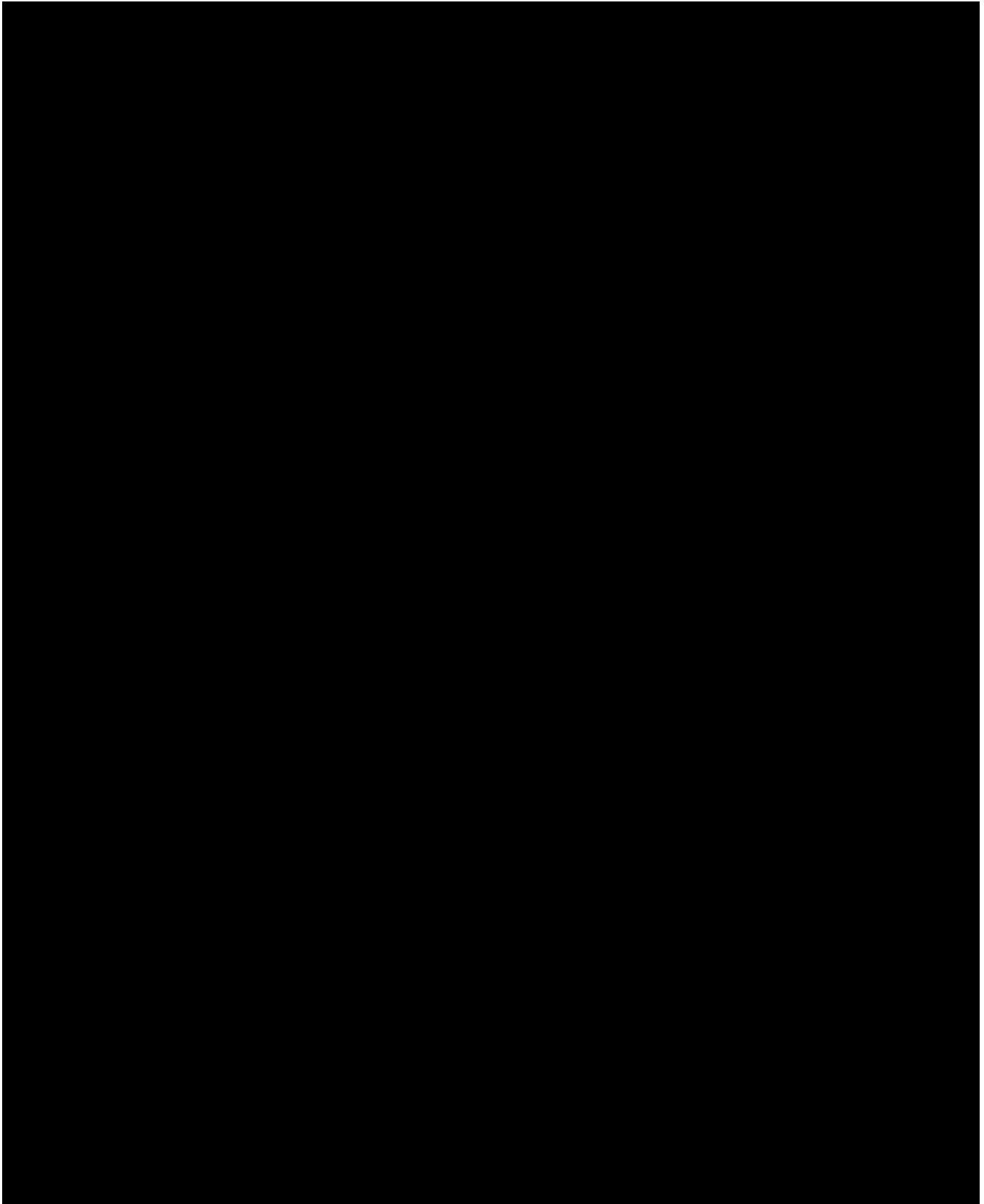


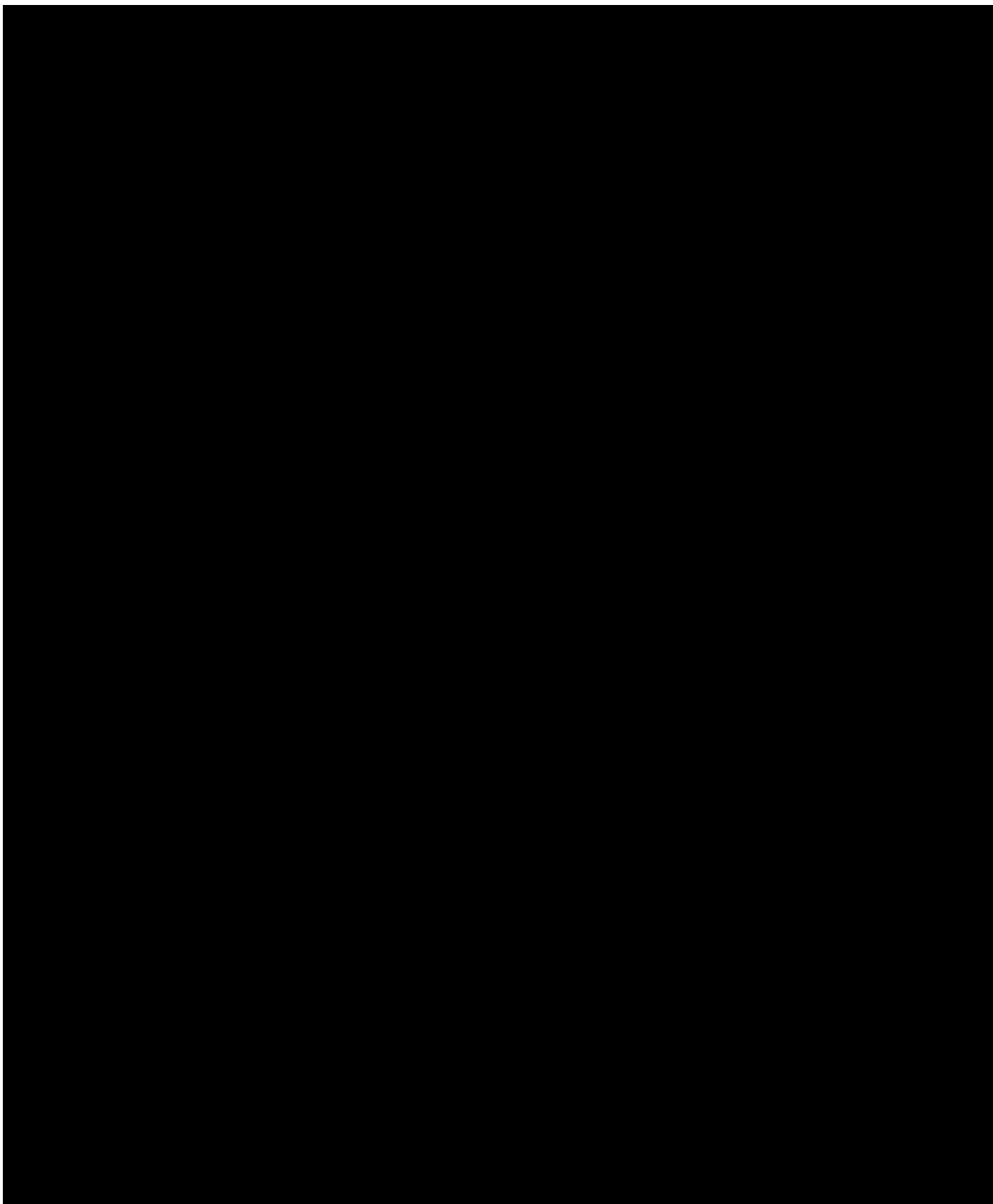


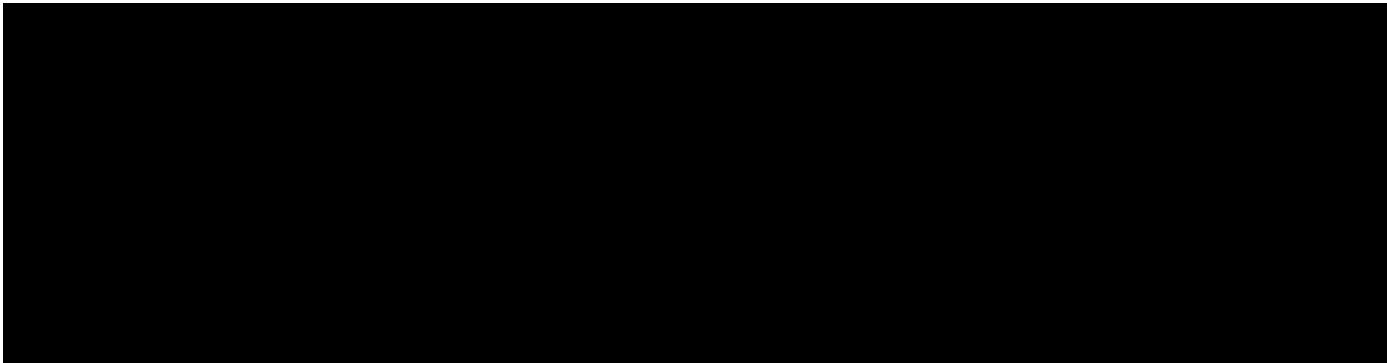
8.9 Latin Version



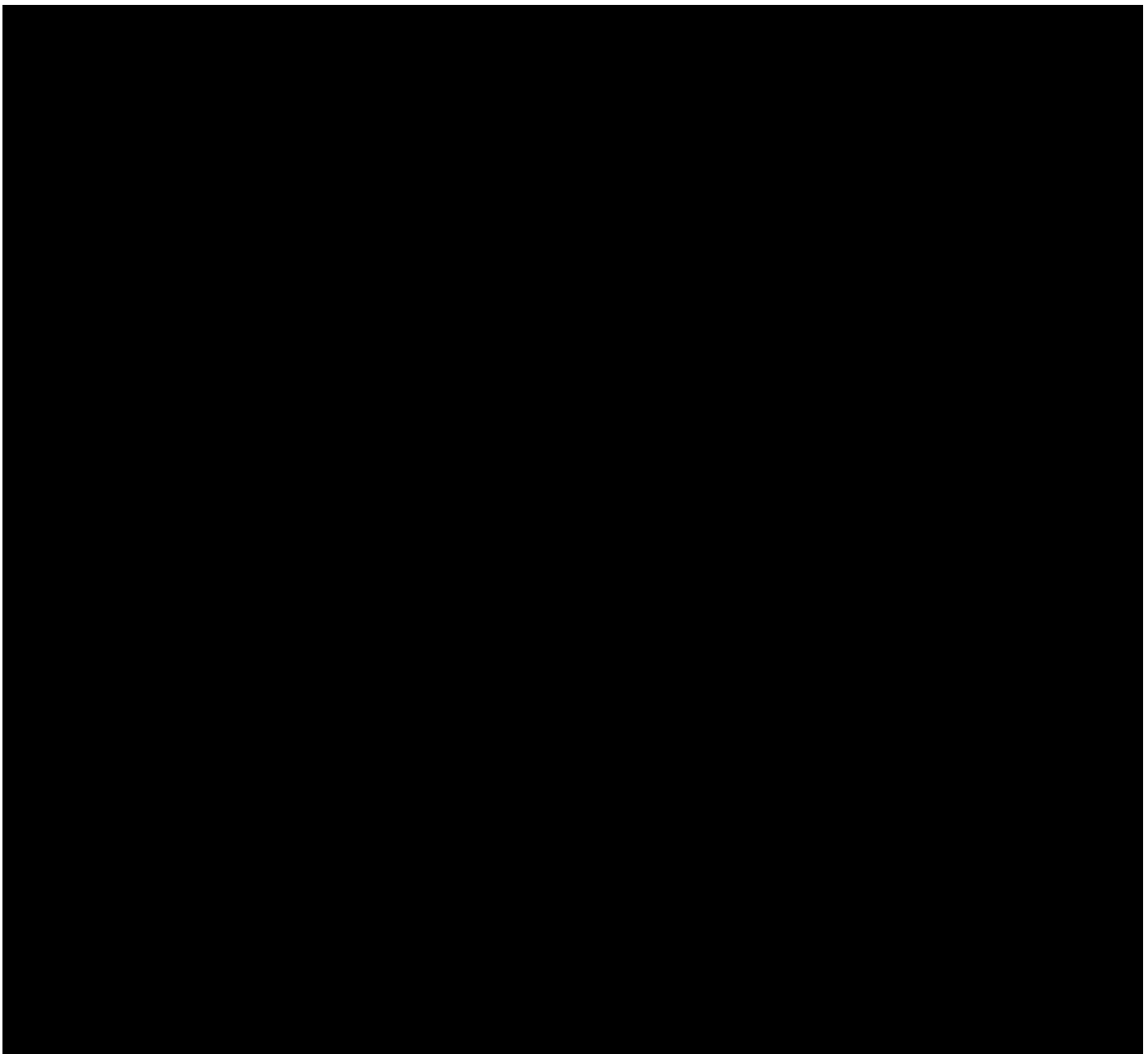


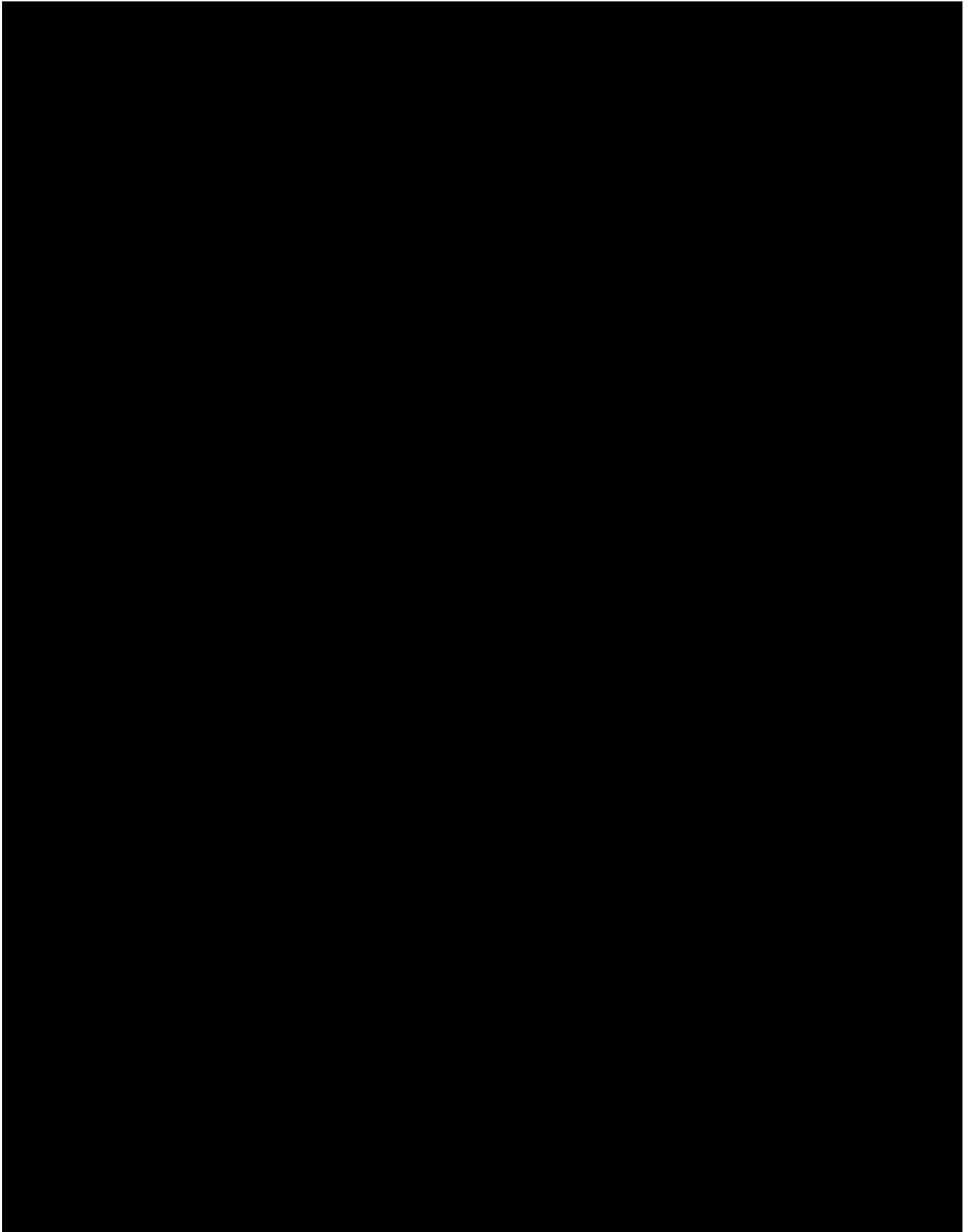


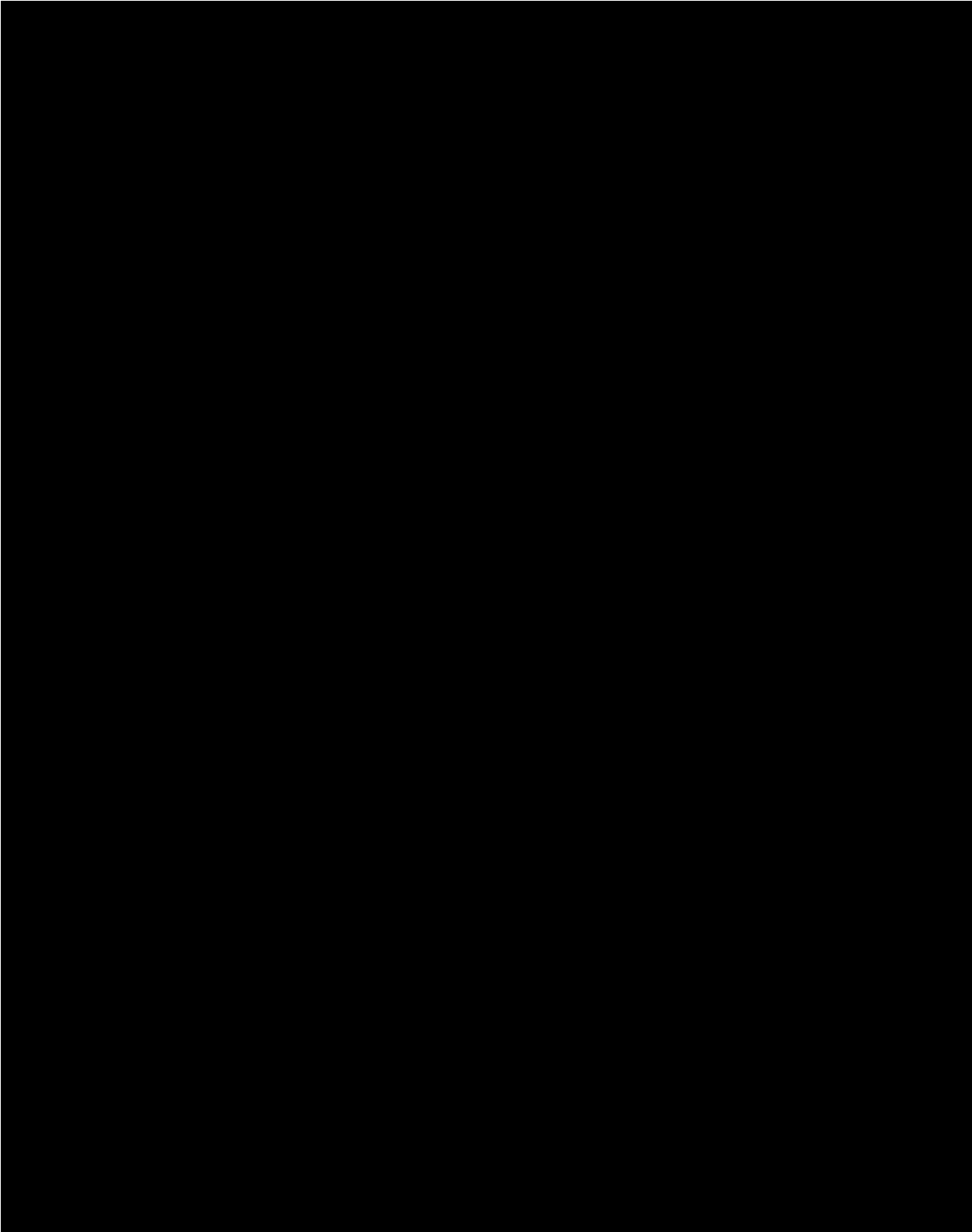


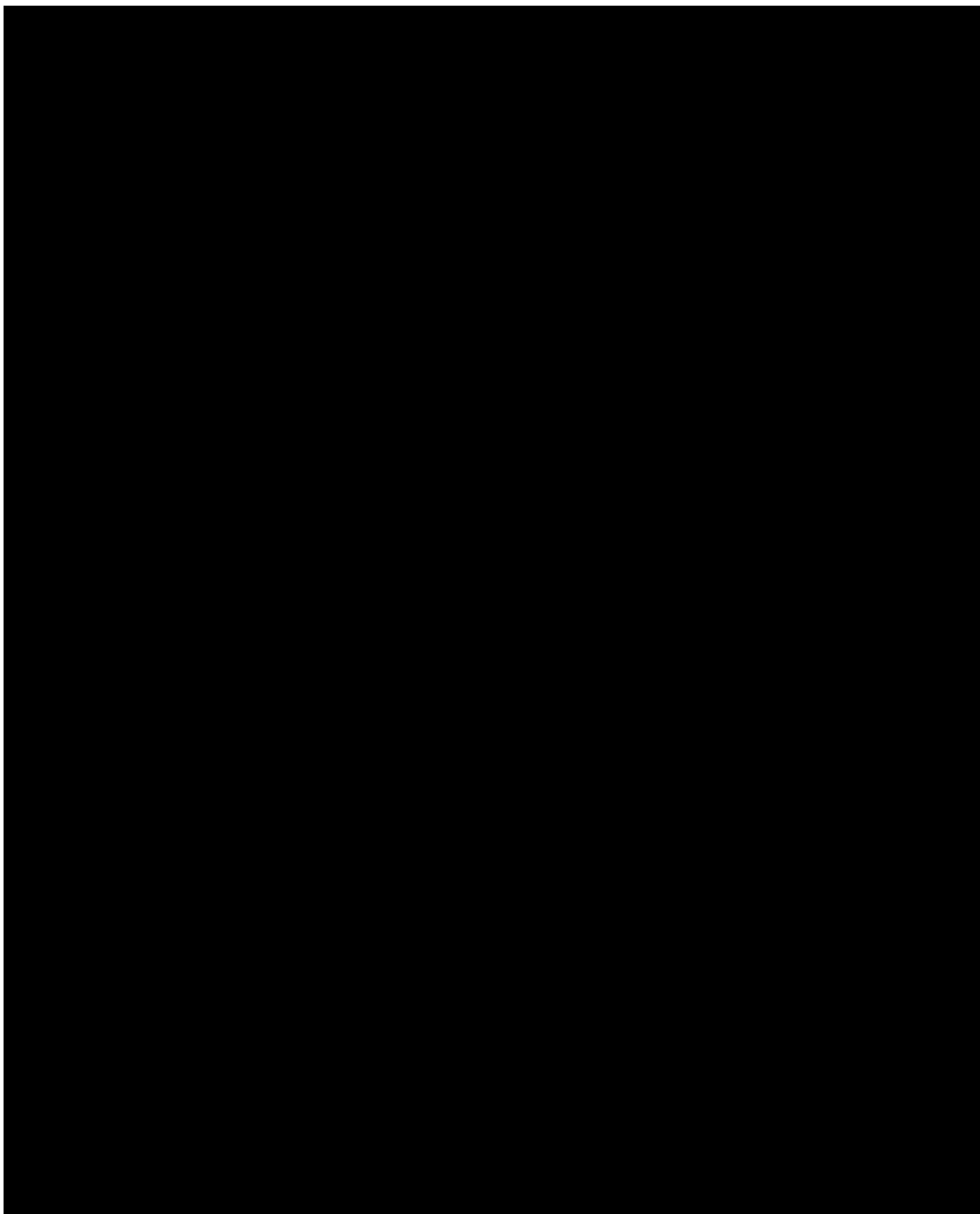


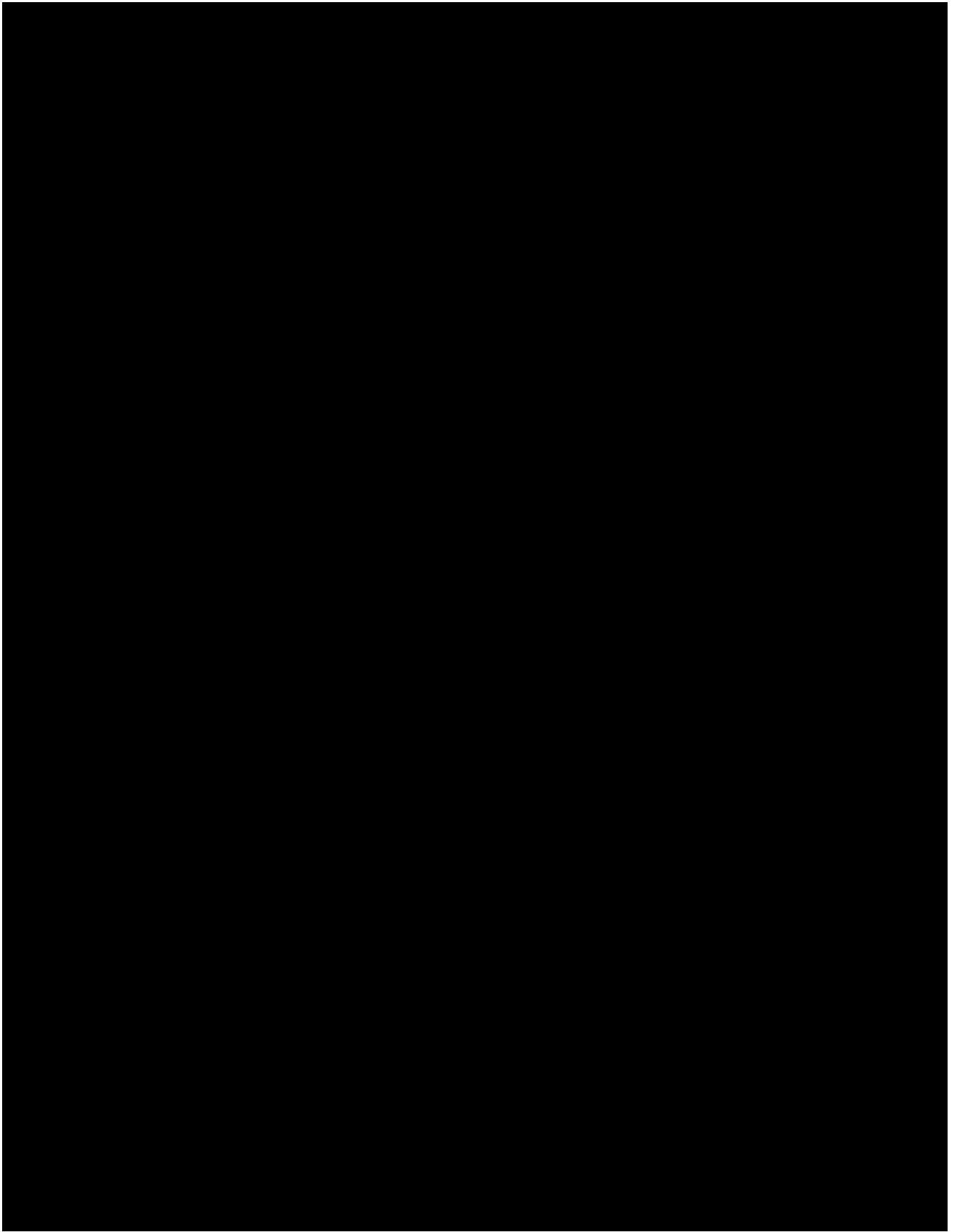
8.10 Greek Version



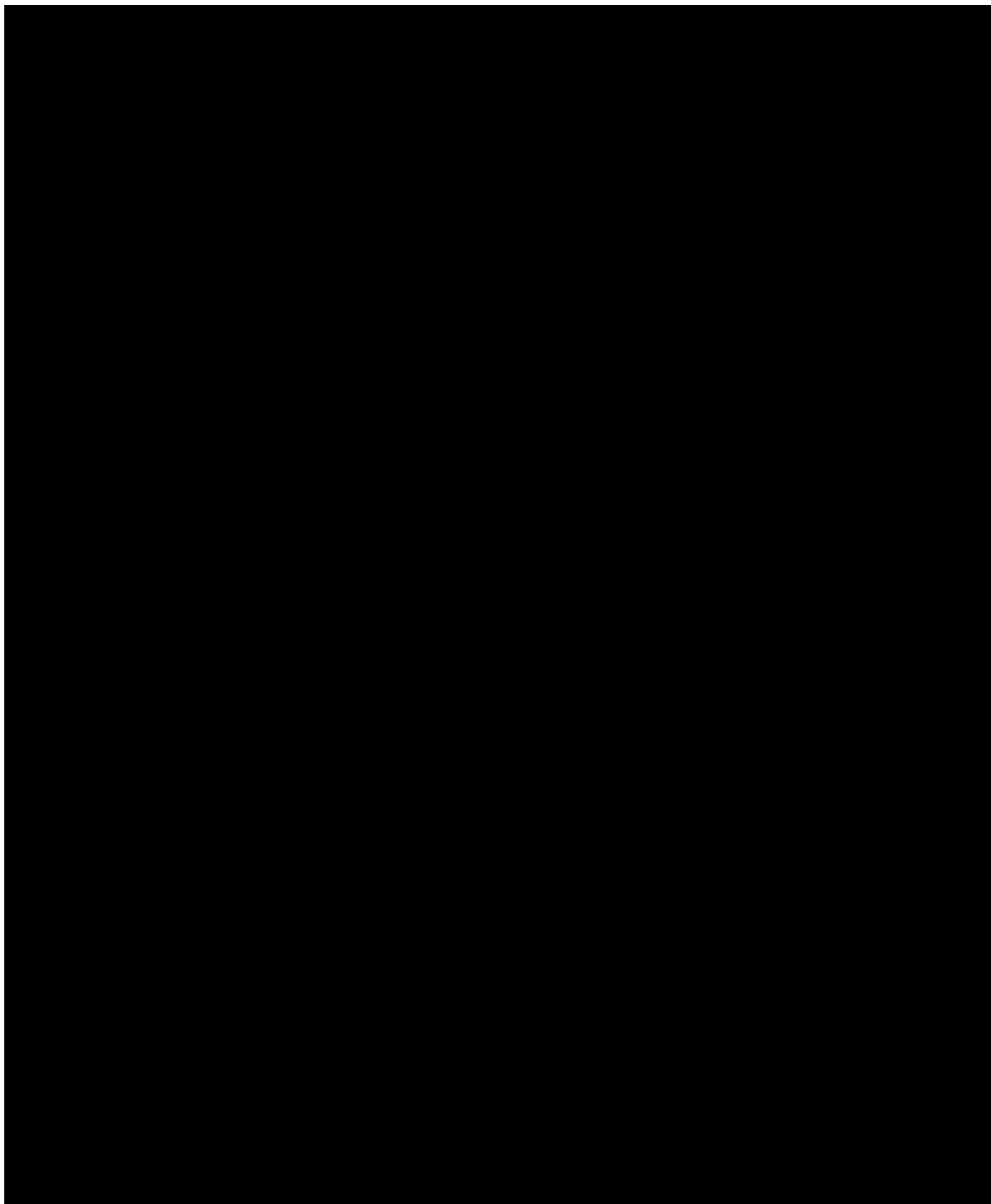


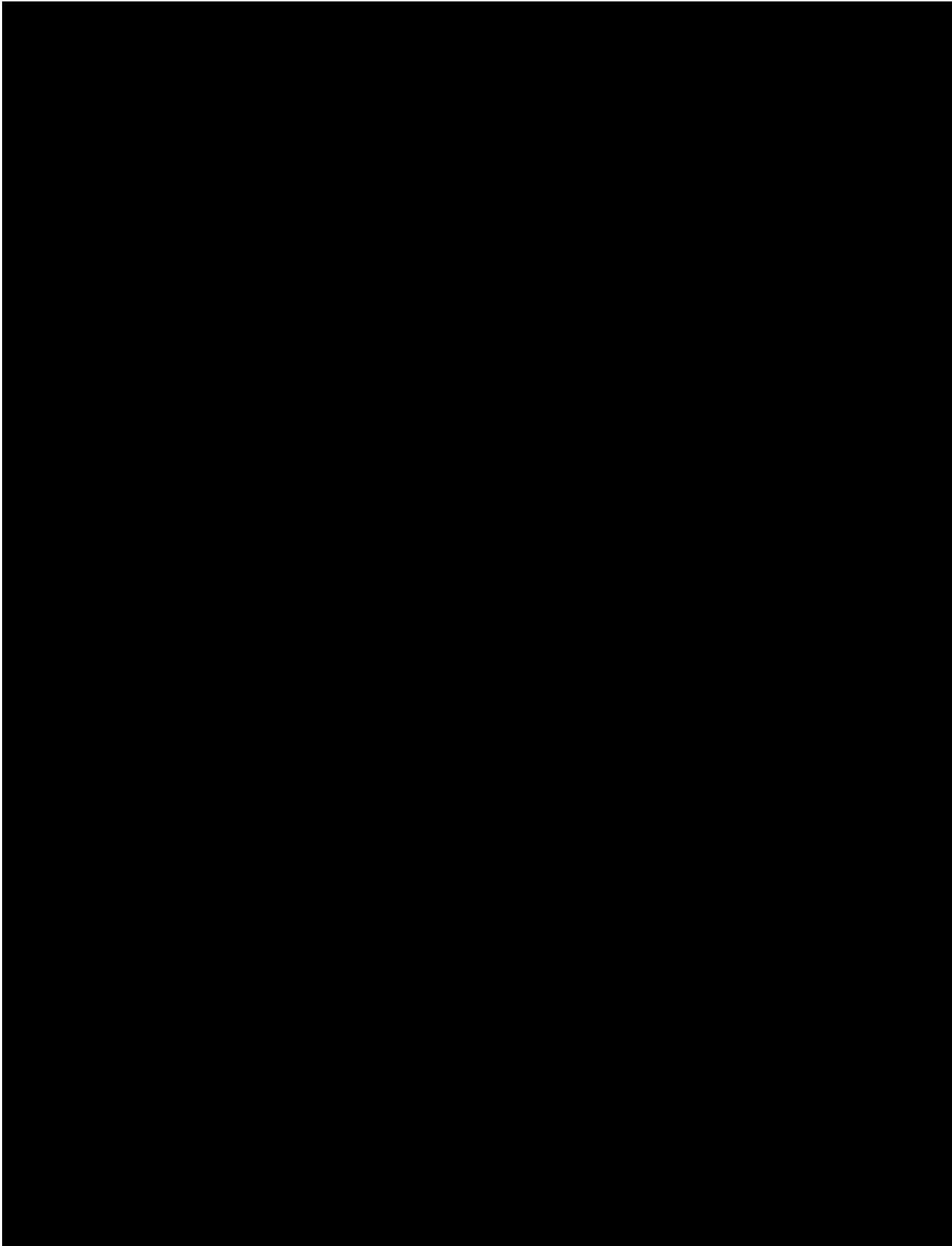


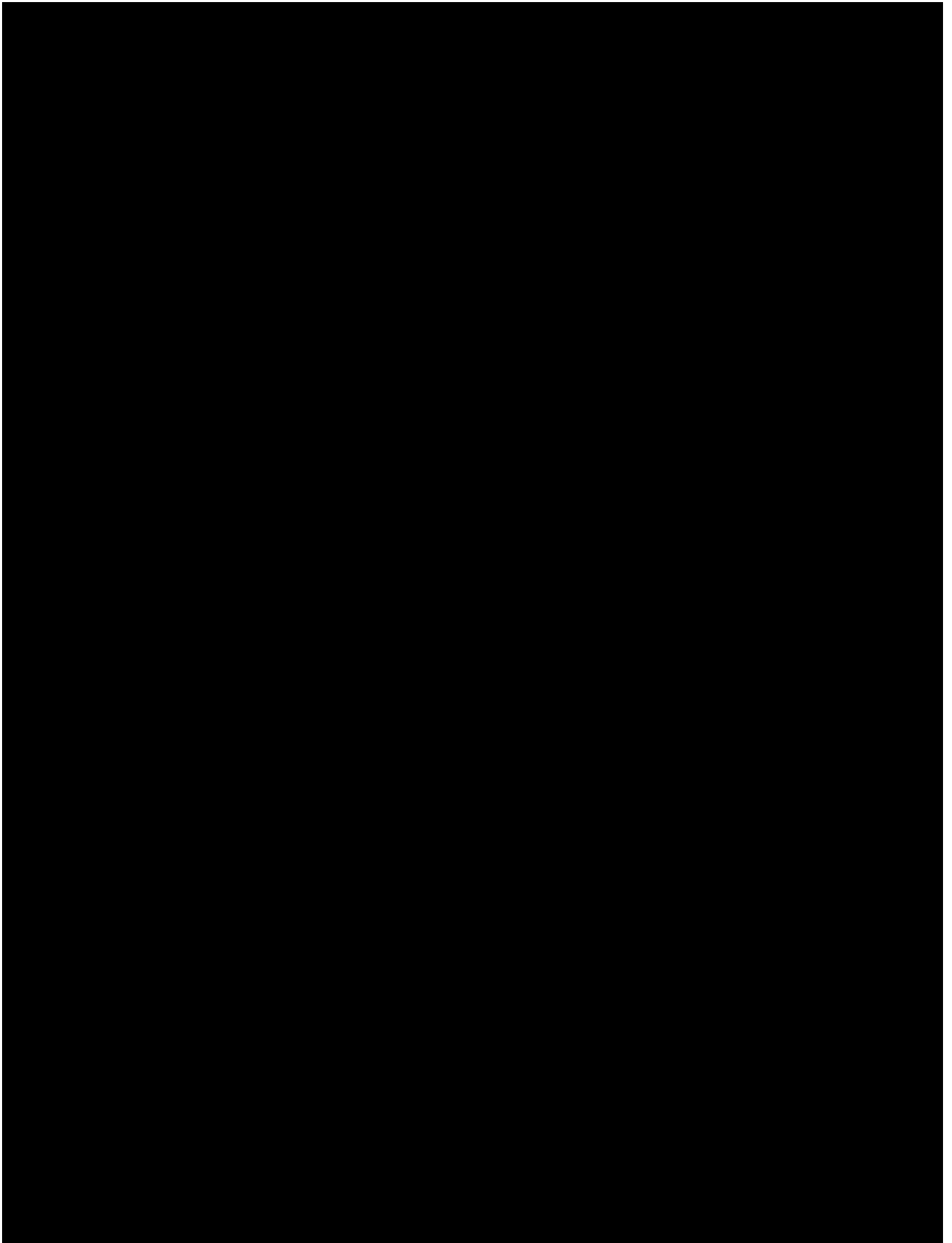


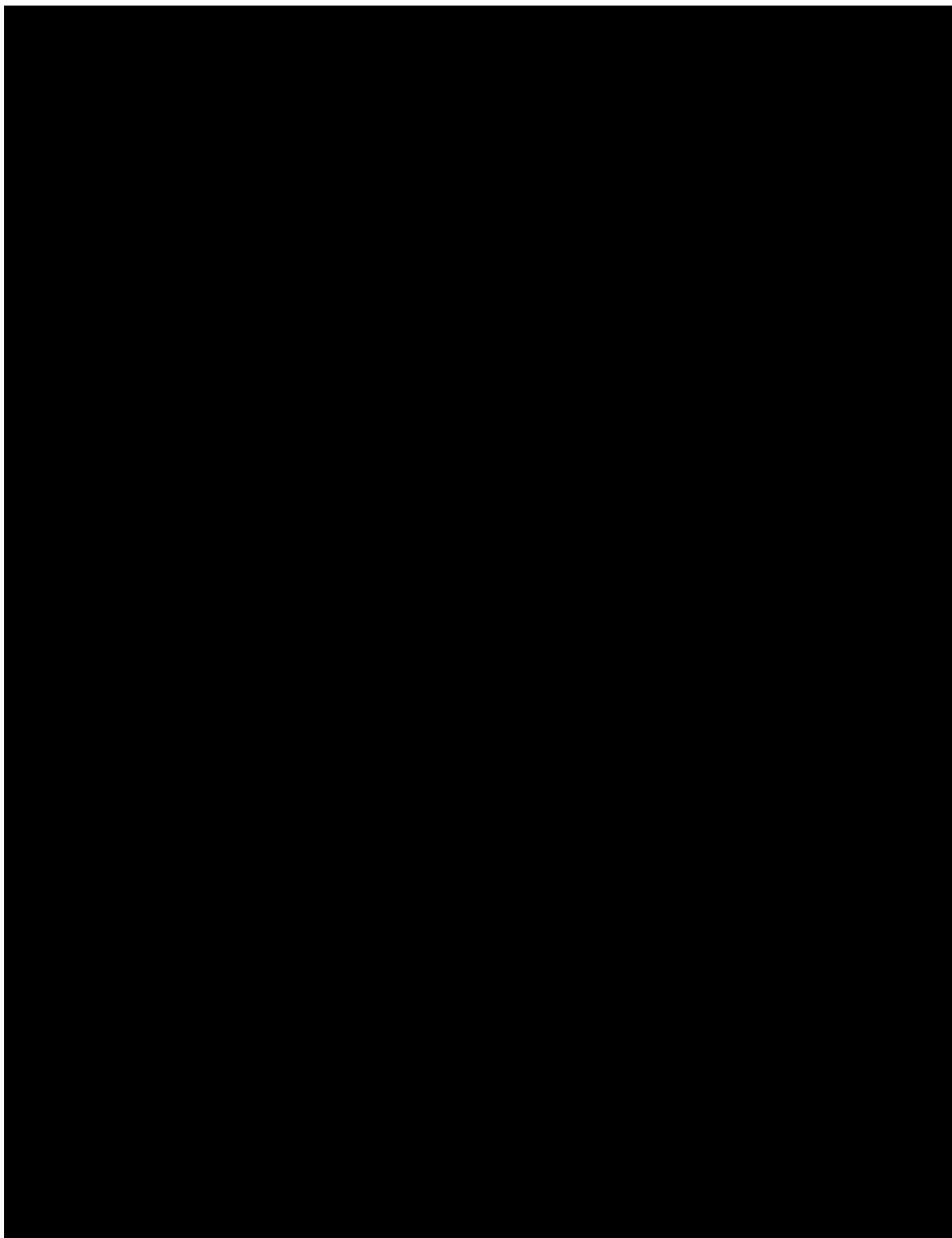


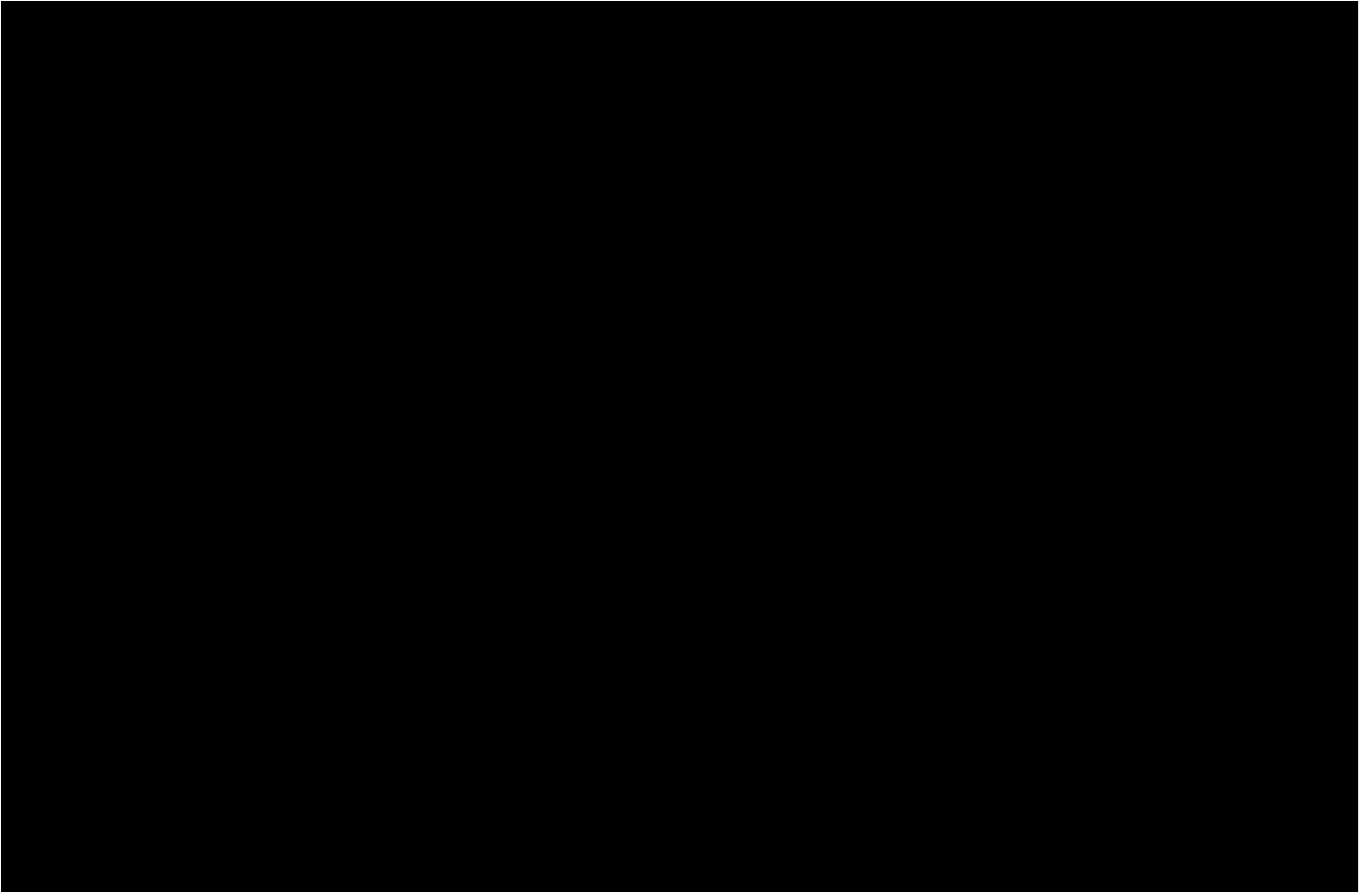
8.11 Croatian Version



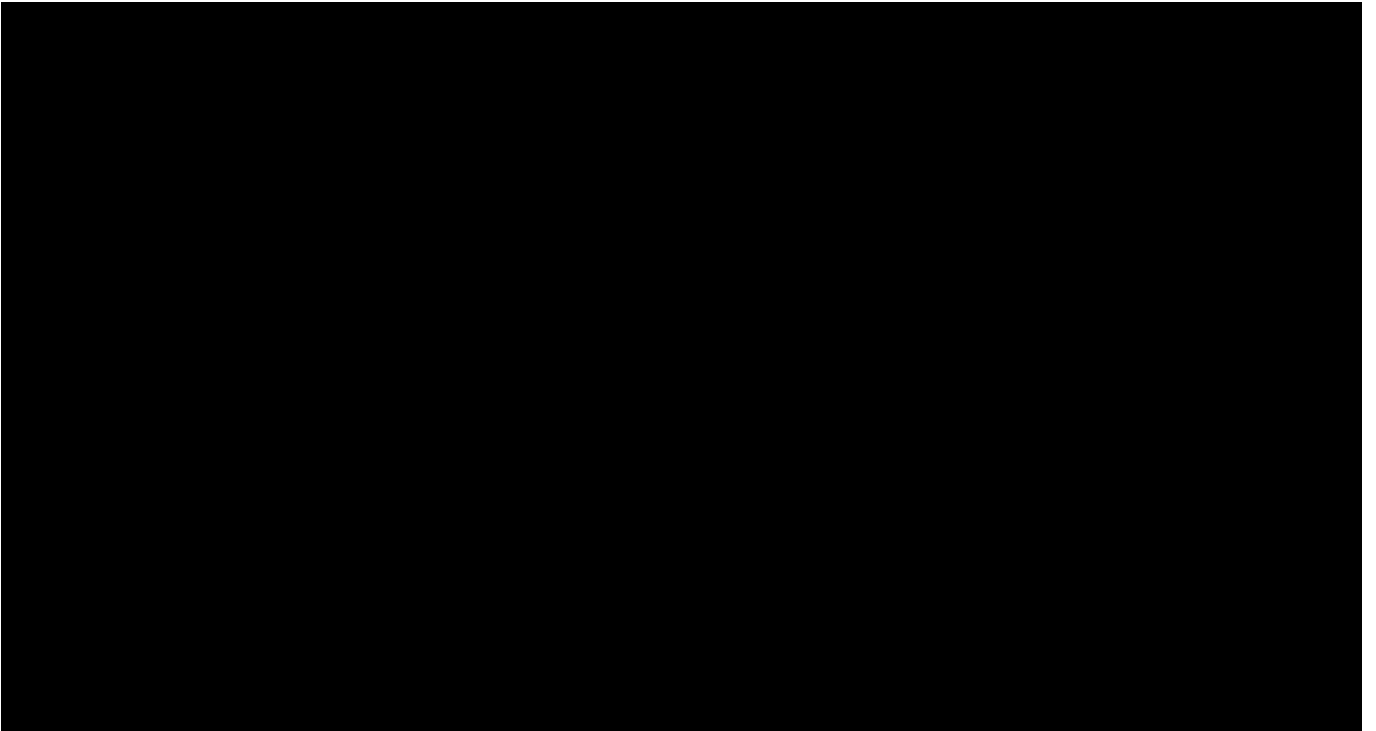


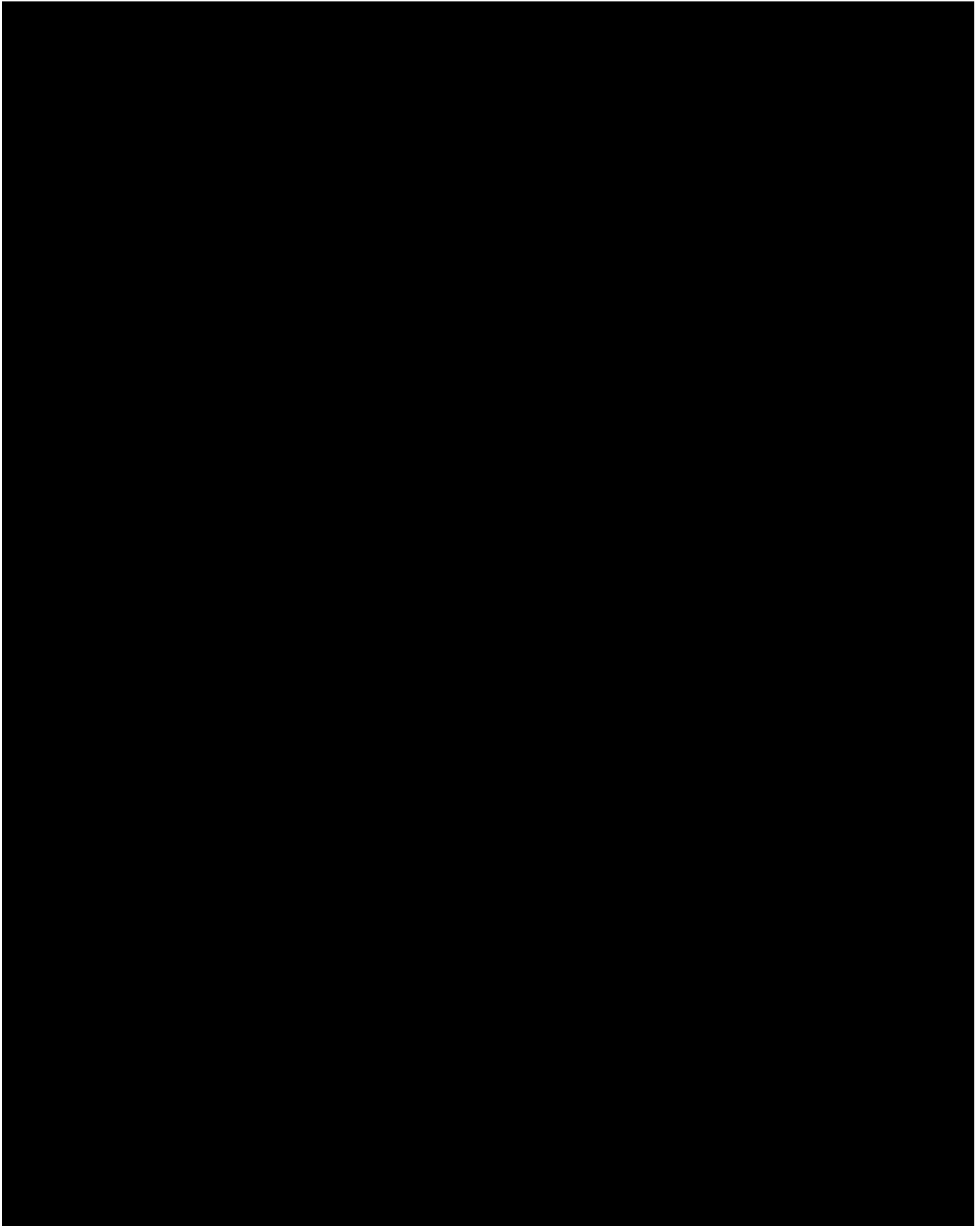


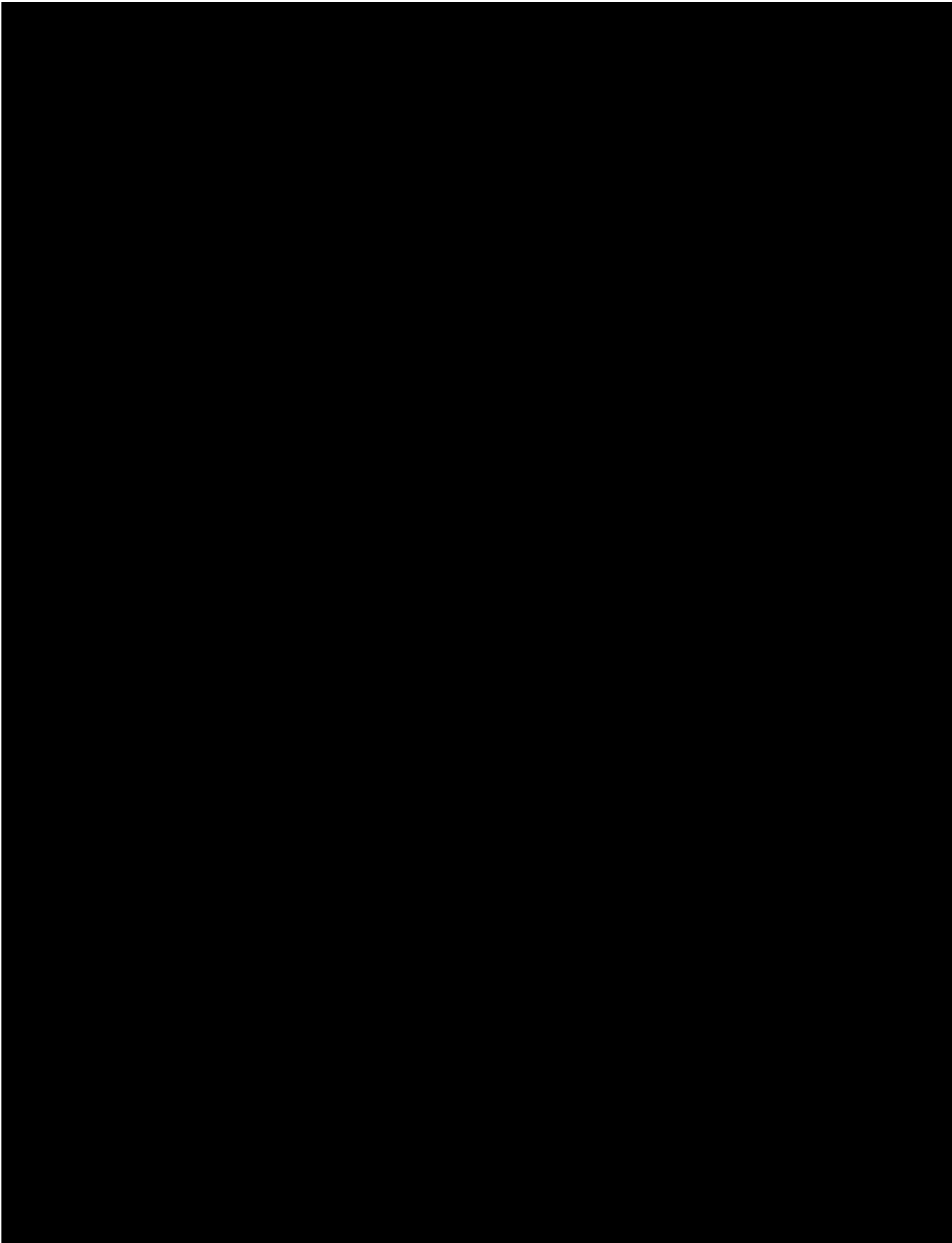


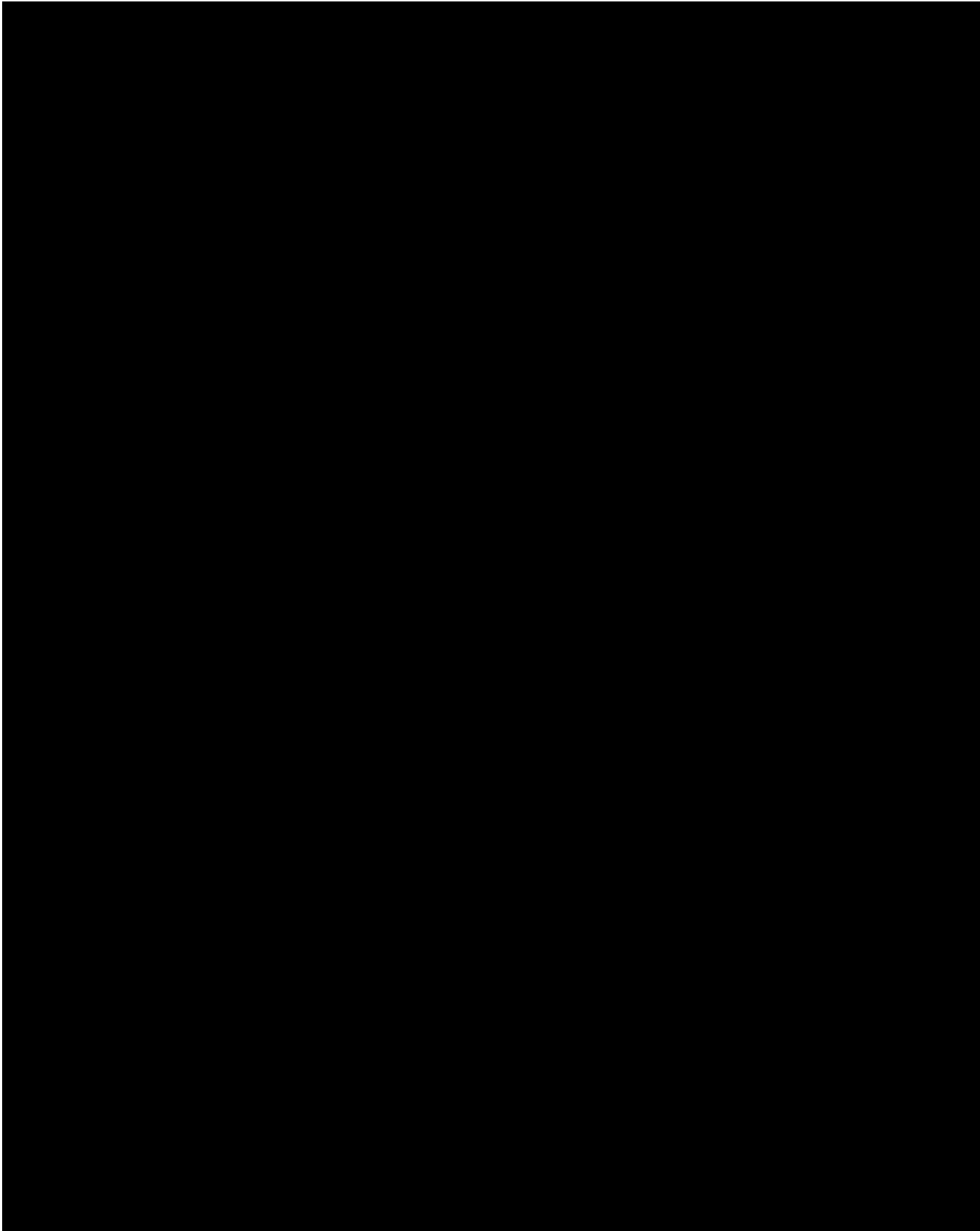


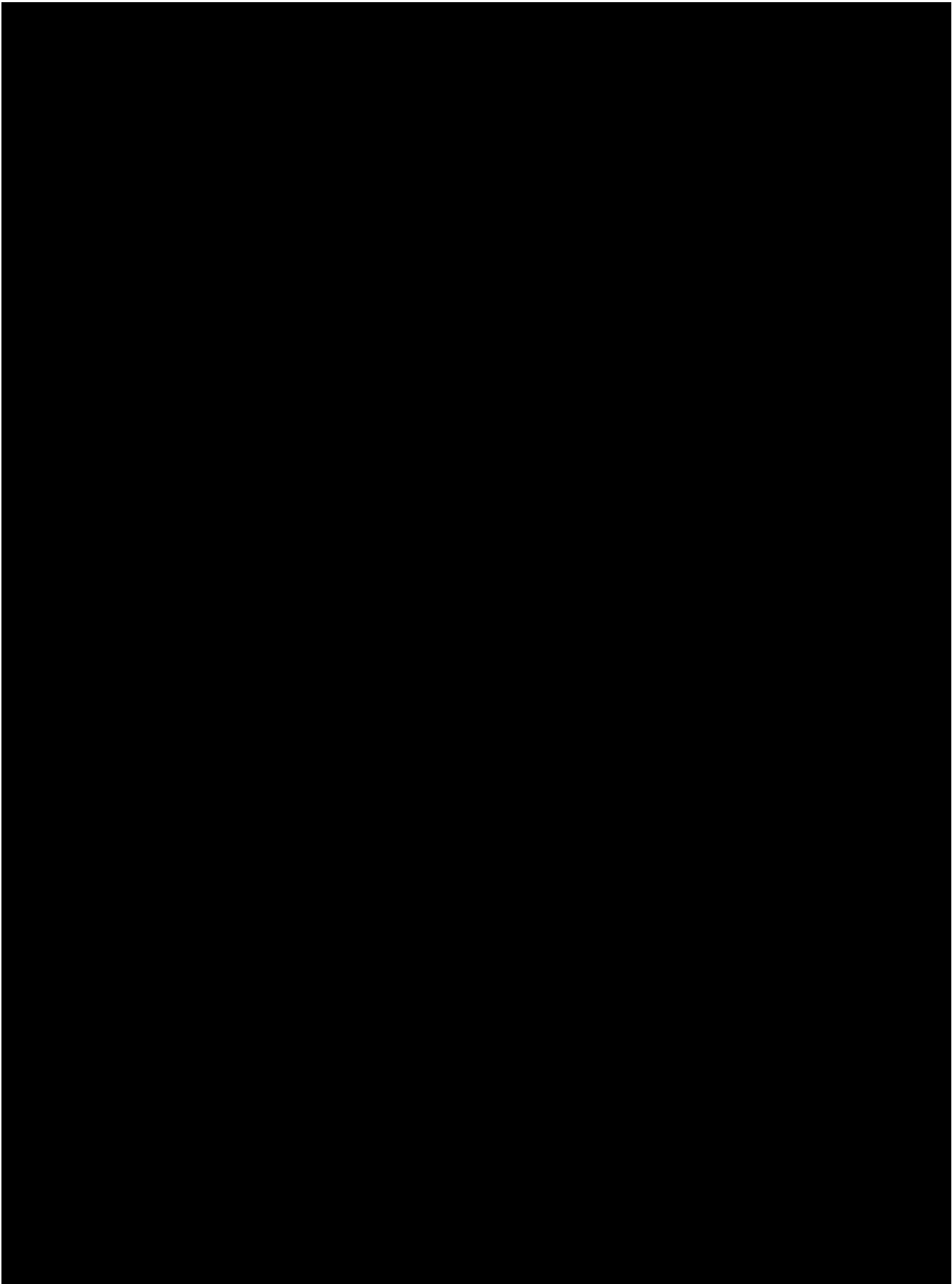
8.12 Turkish Version











9 Appendix B Leaflet Readability Methodology.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

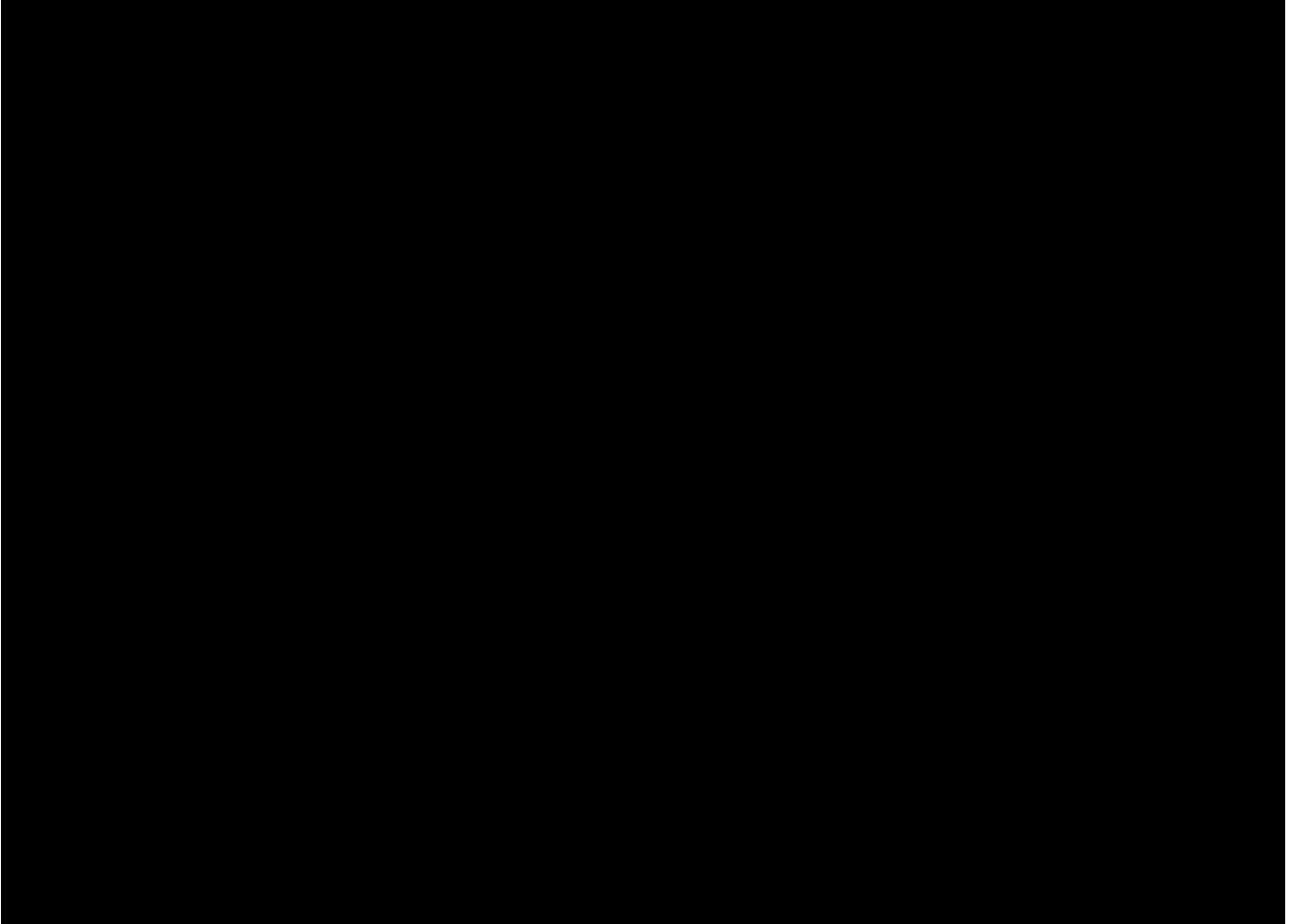
[REDACTED]

[REDACTED]

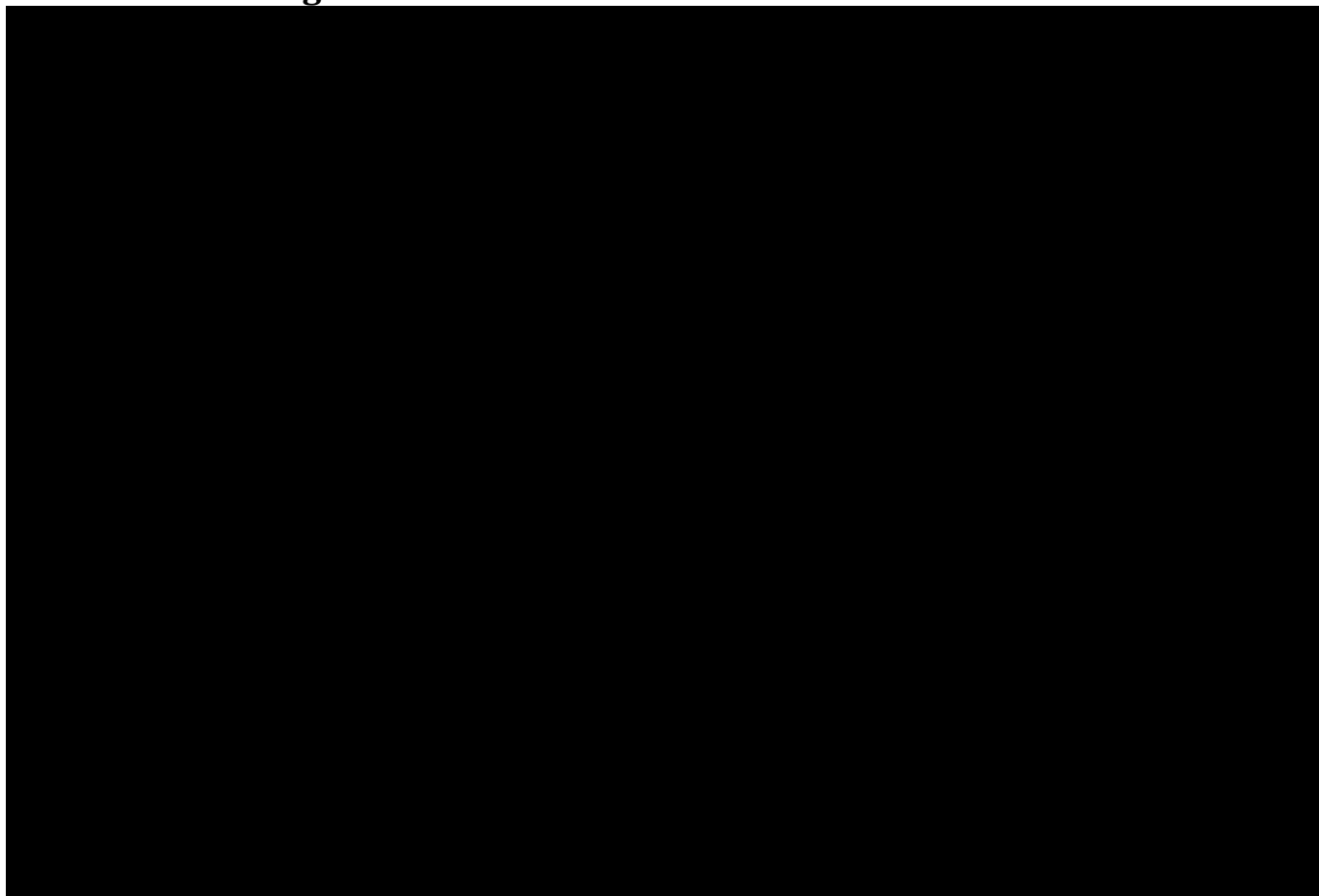
[REDACTED]

10 Appendix C Travellers Leaflet

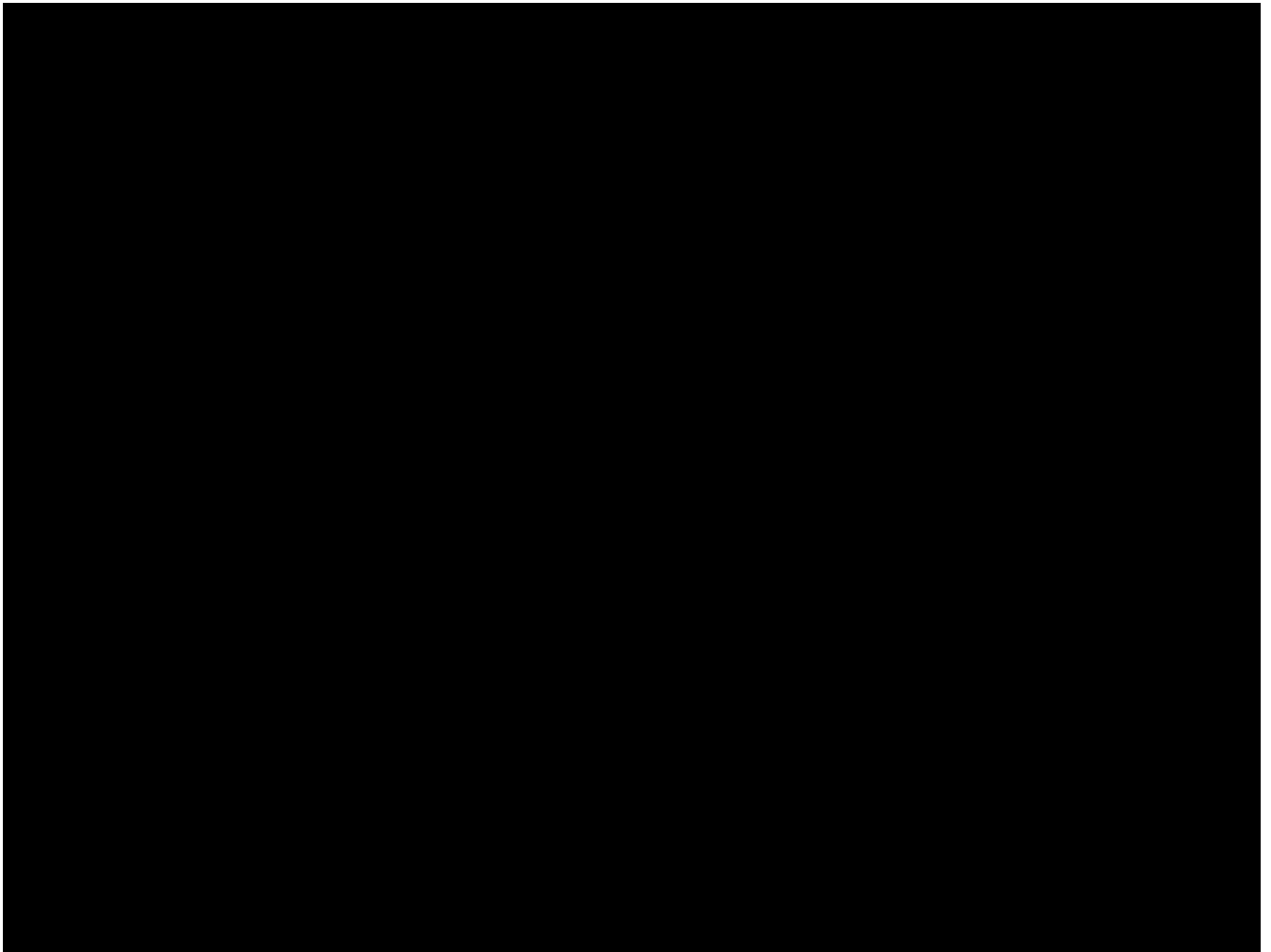
10.1 English Version



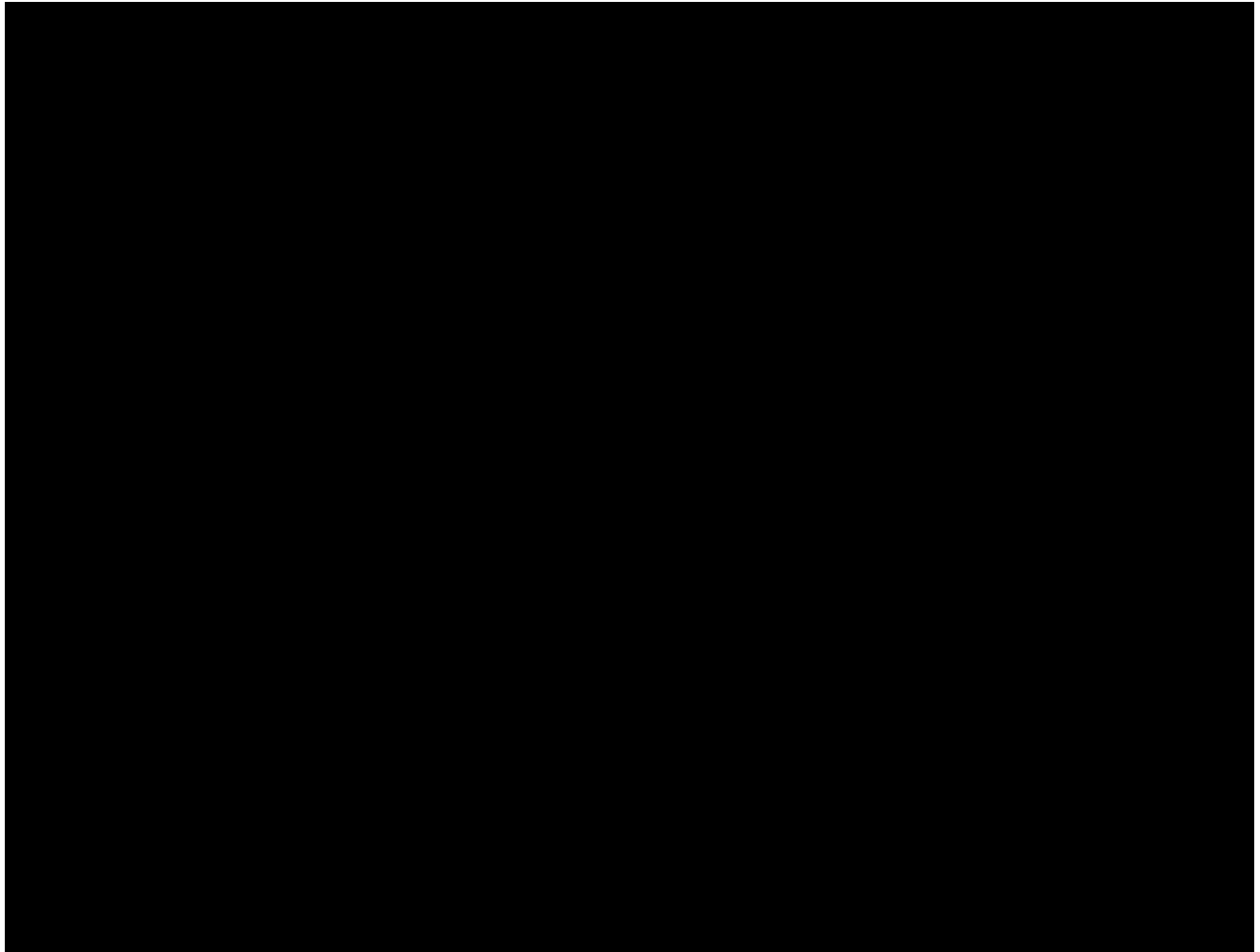
10.2 Hungarian Version



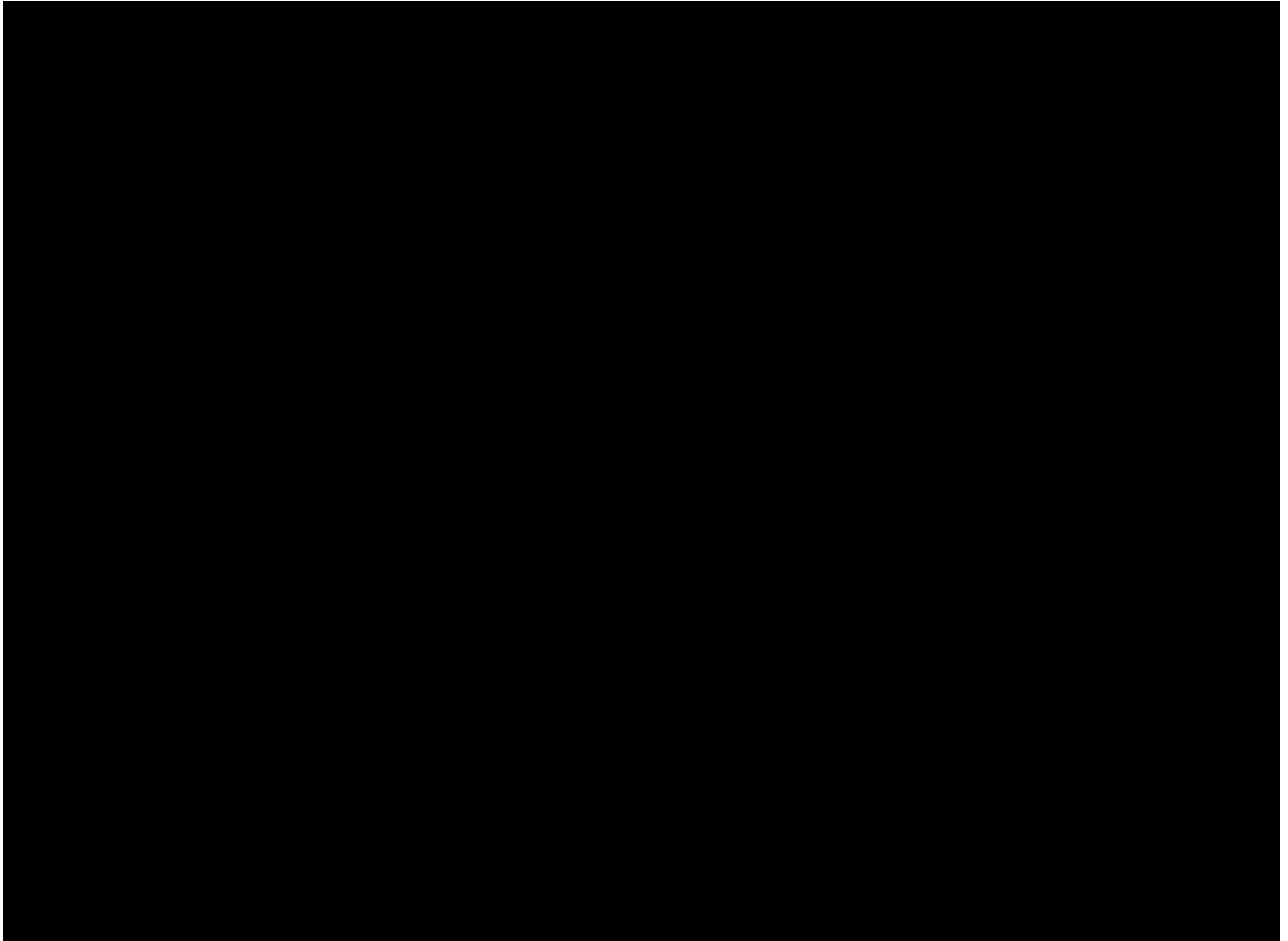
10.3 Serbian Version



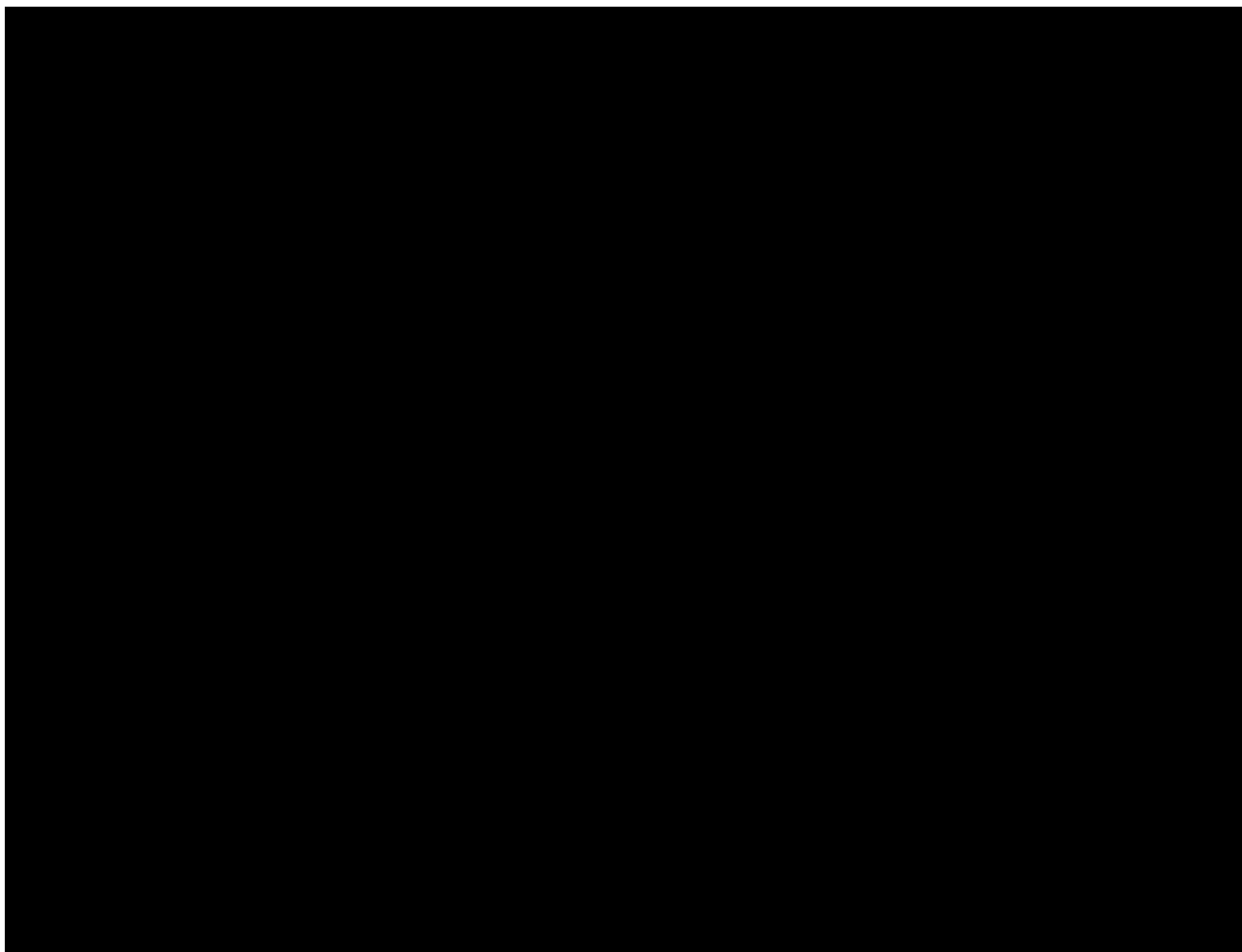
10.4 German Version



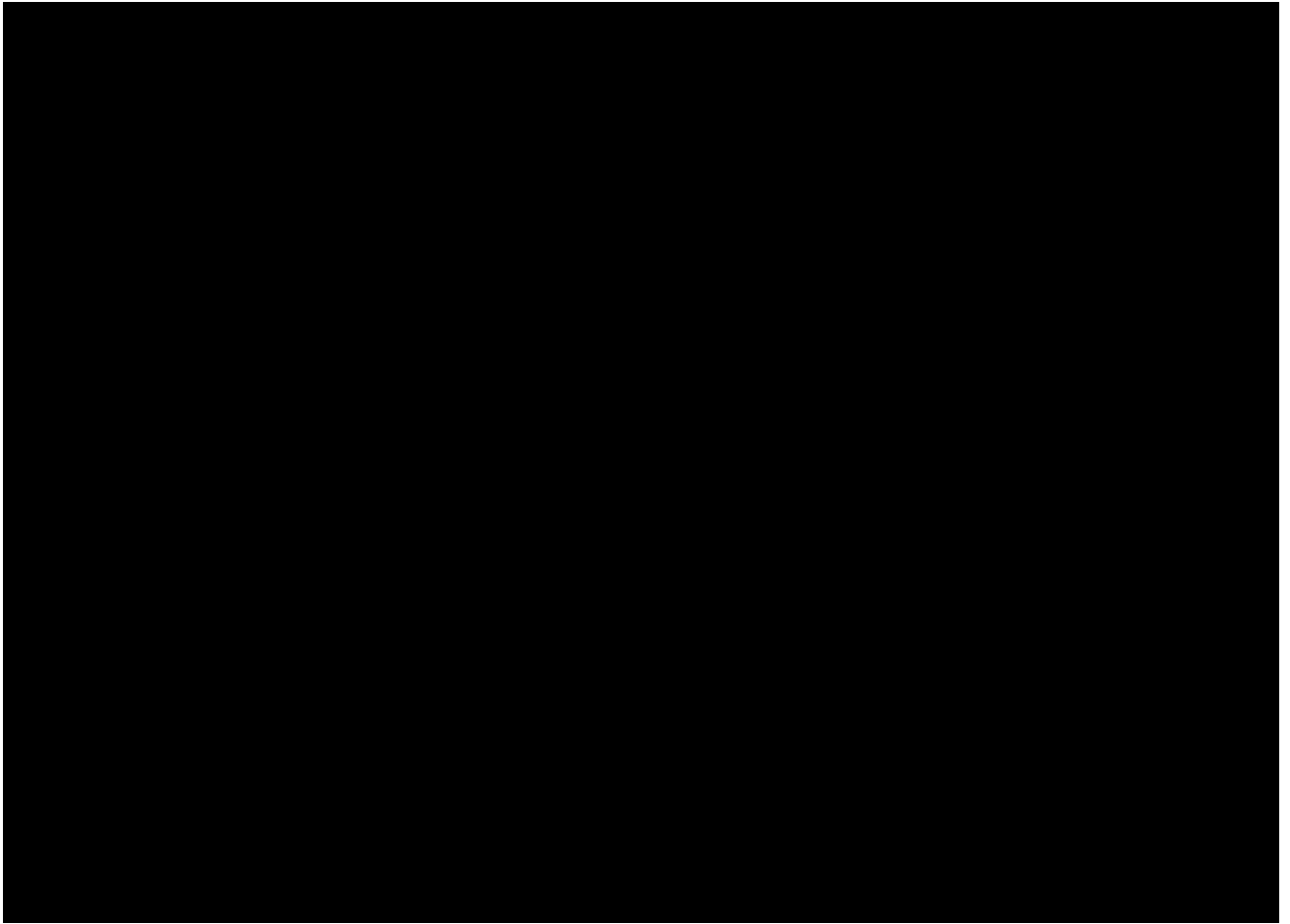
10.5 Arabic Version



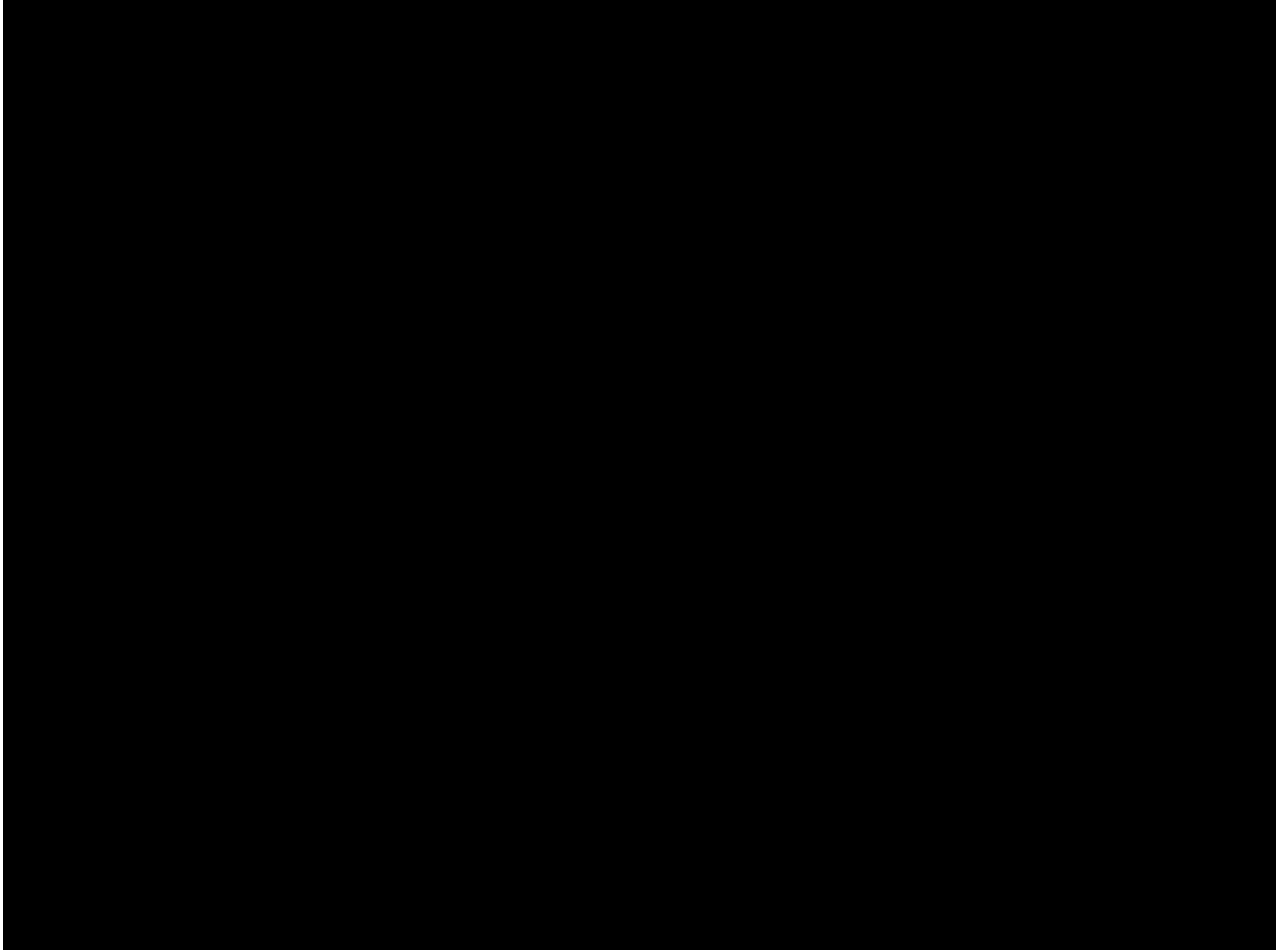
10.6 Spanish Version



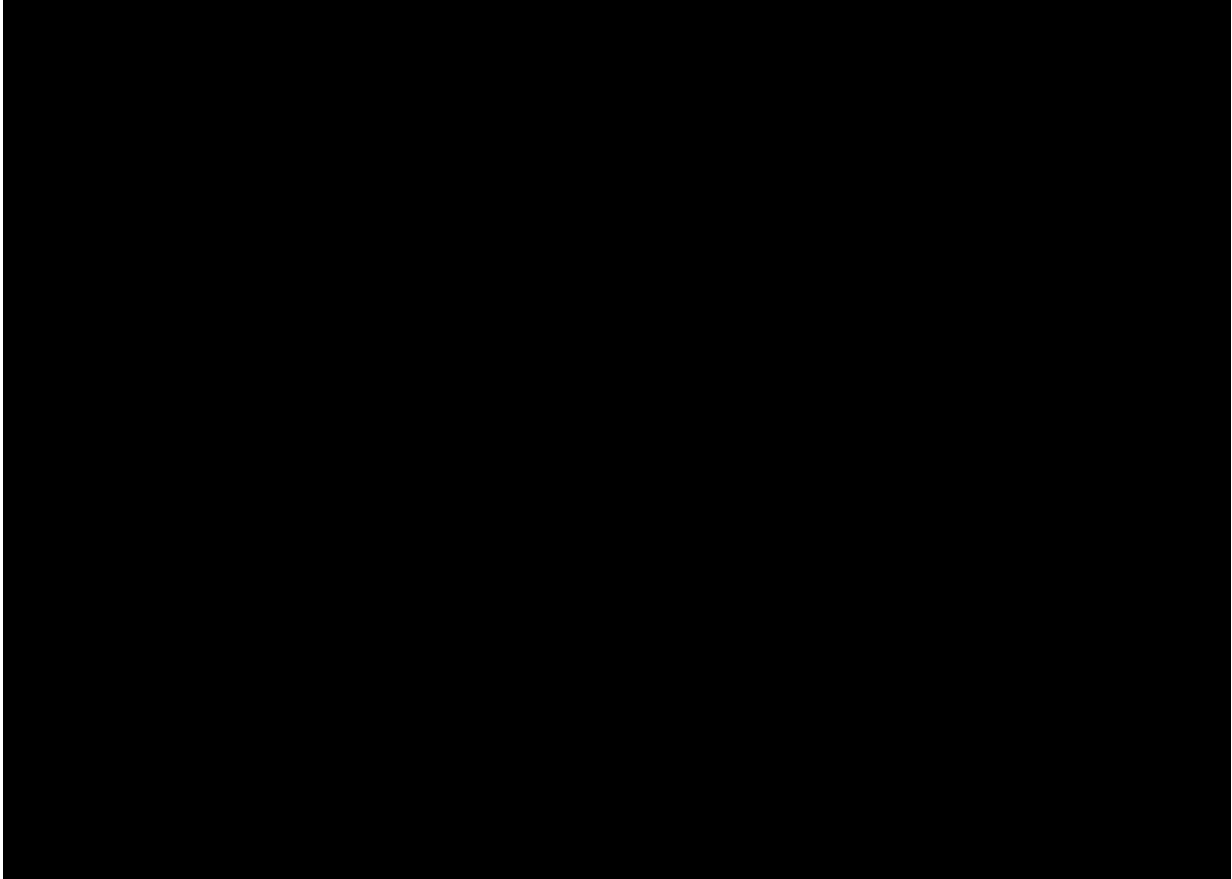
10.7 Russian Version



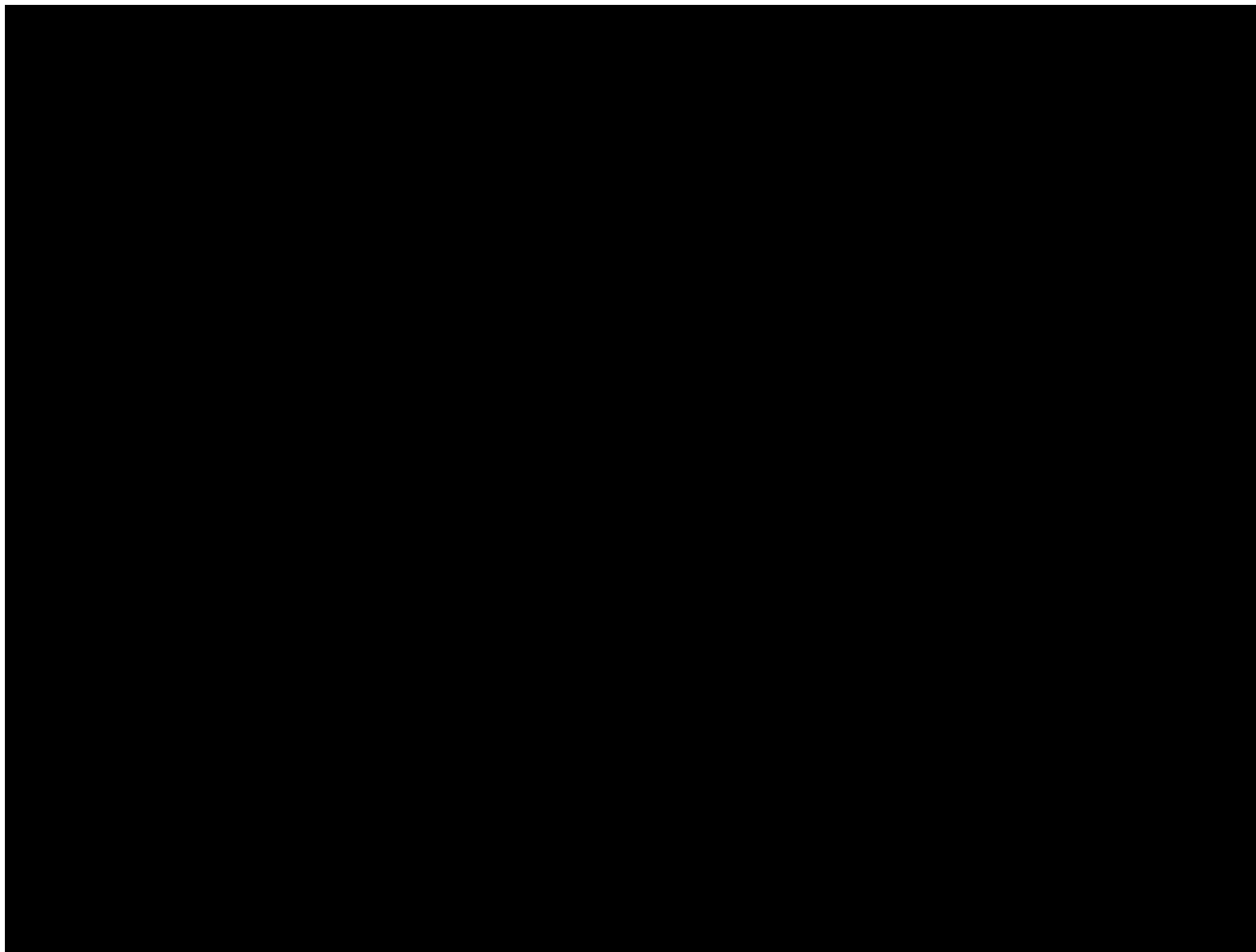
10.8 Greek Version



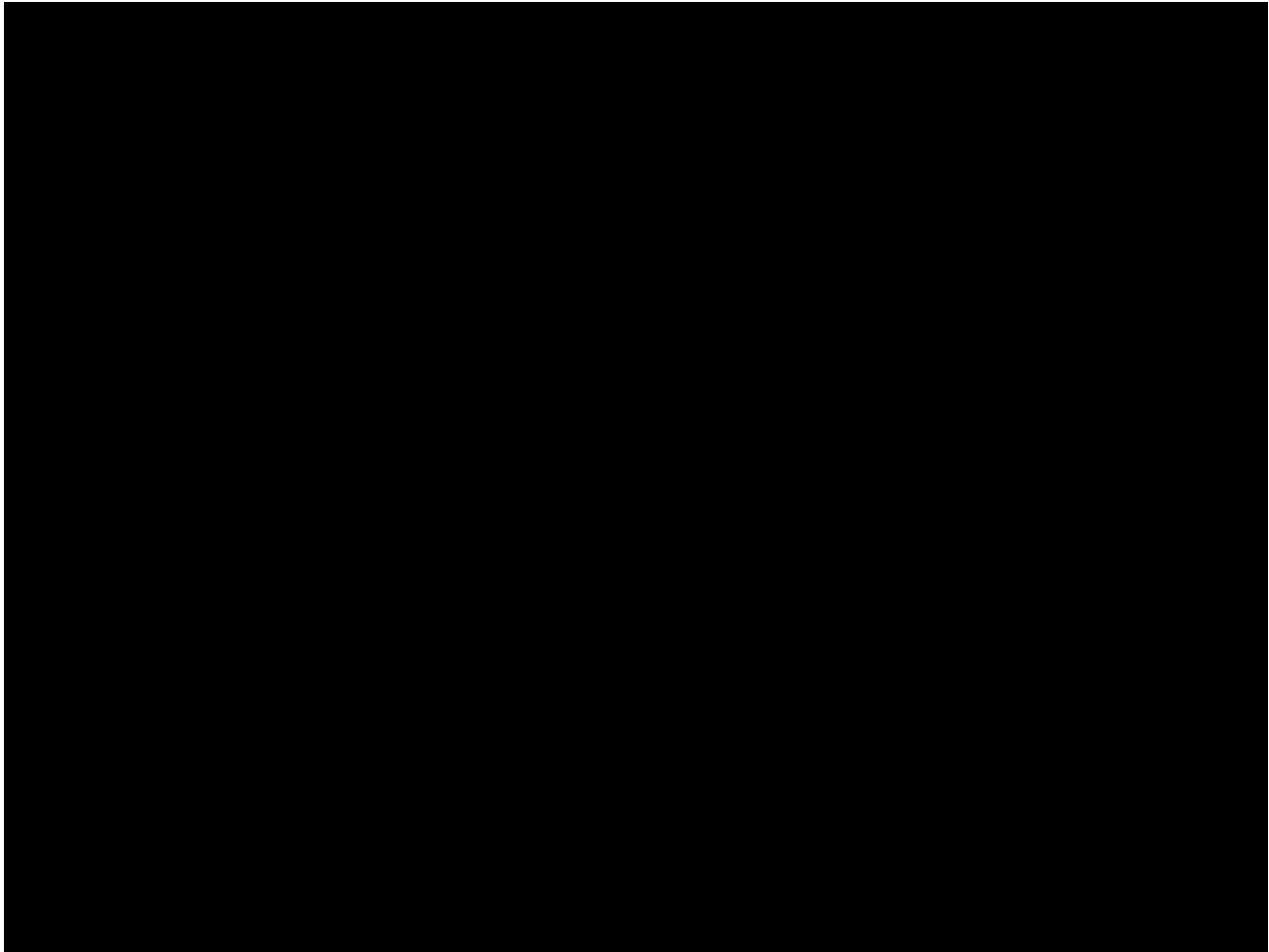
10.9 Latin Version



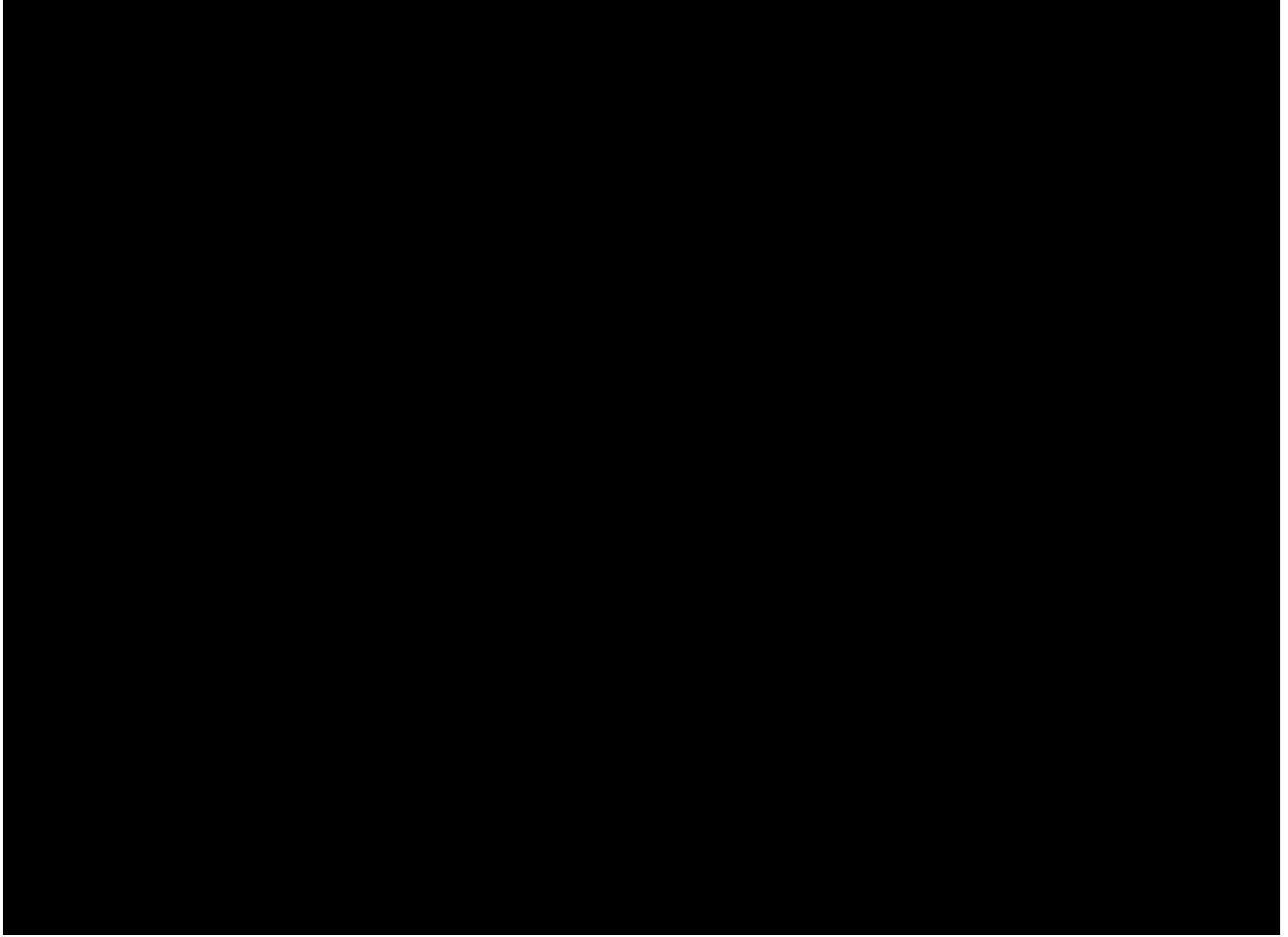
10.10 Chinese Version



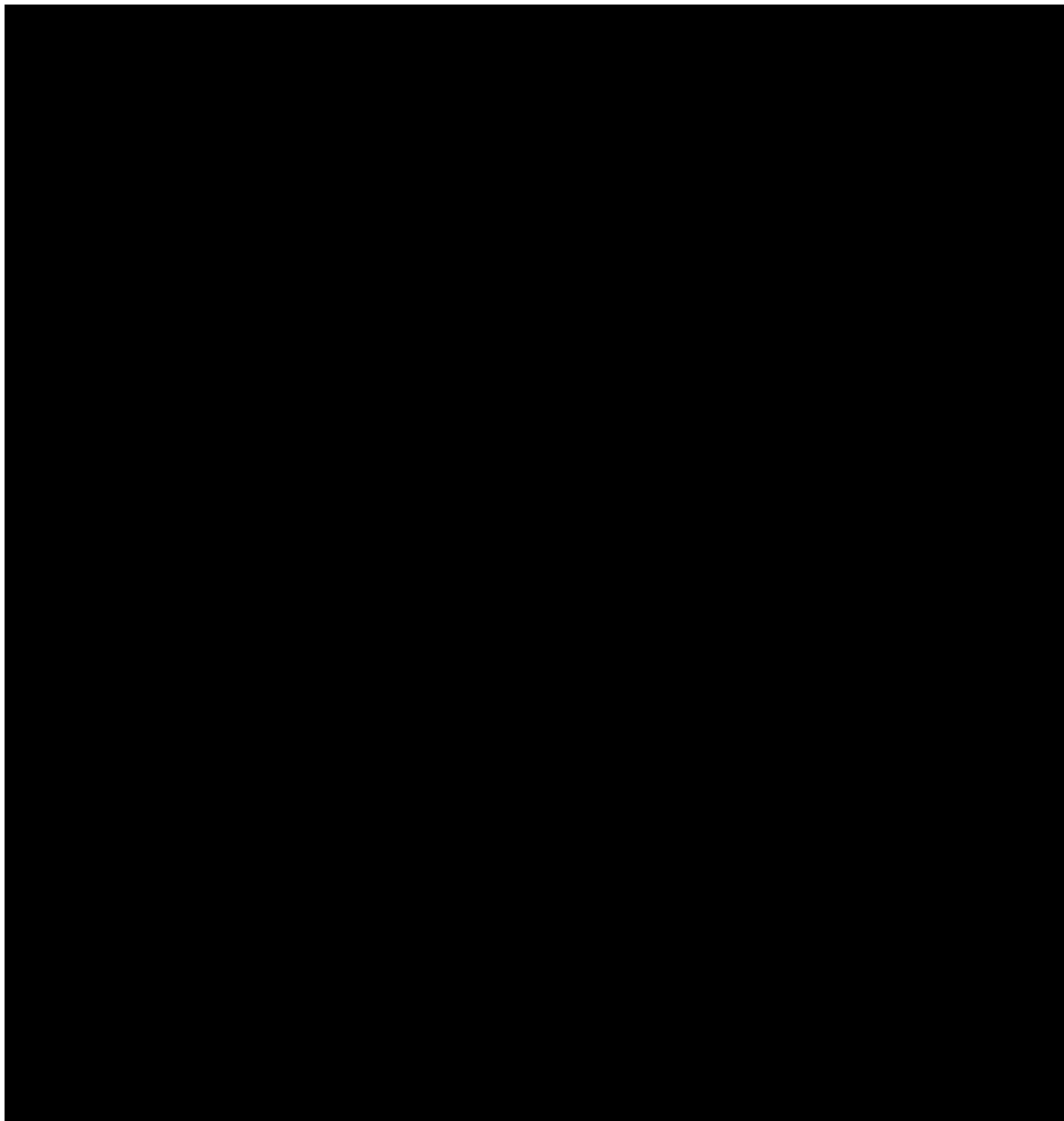
10.11 French Version

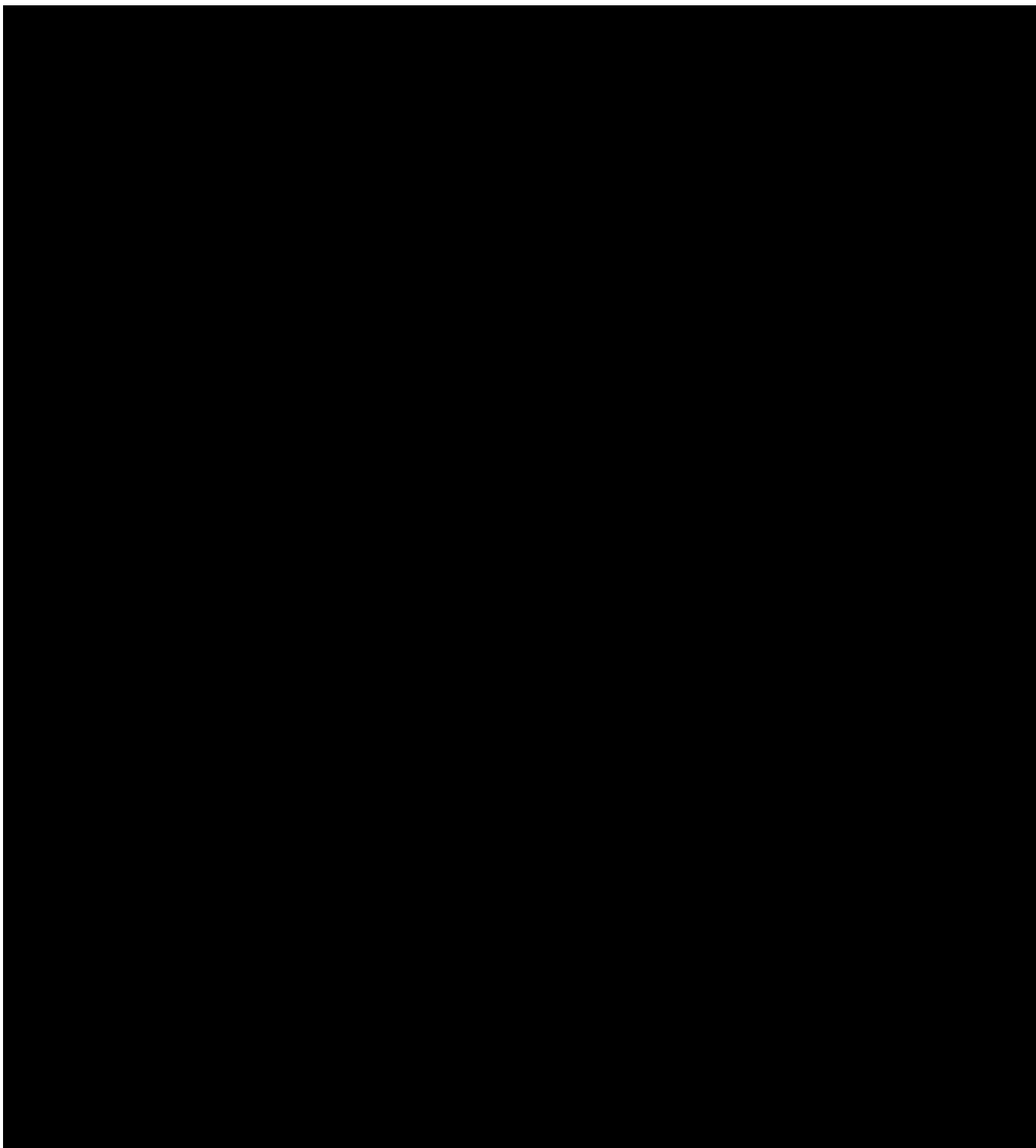


10.12 Turkish version



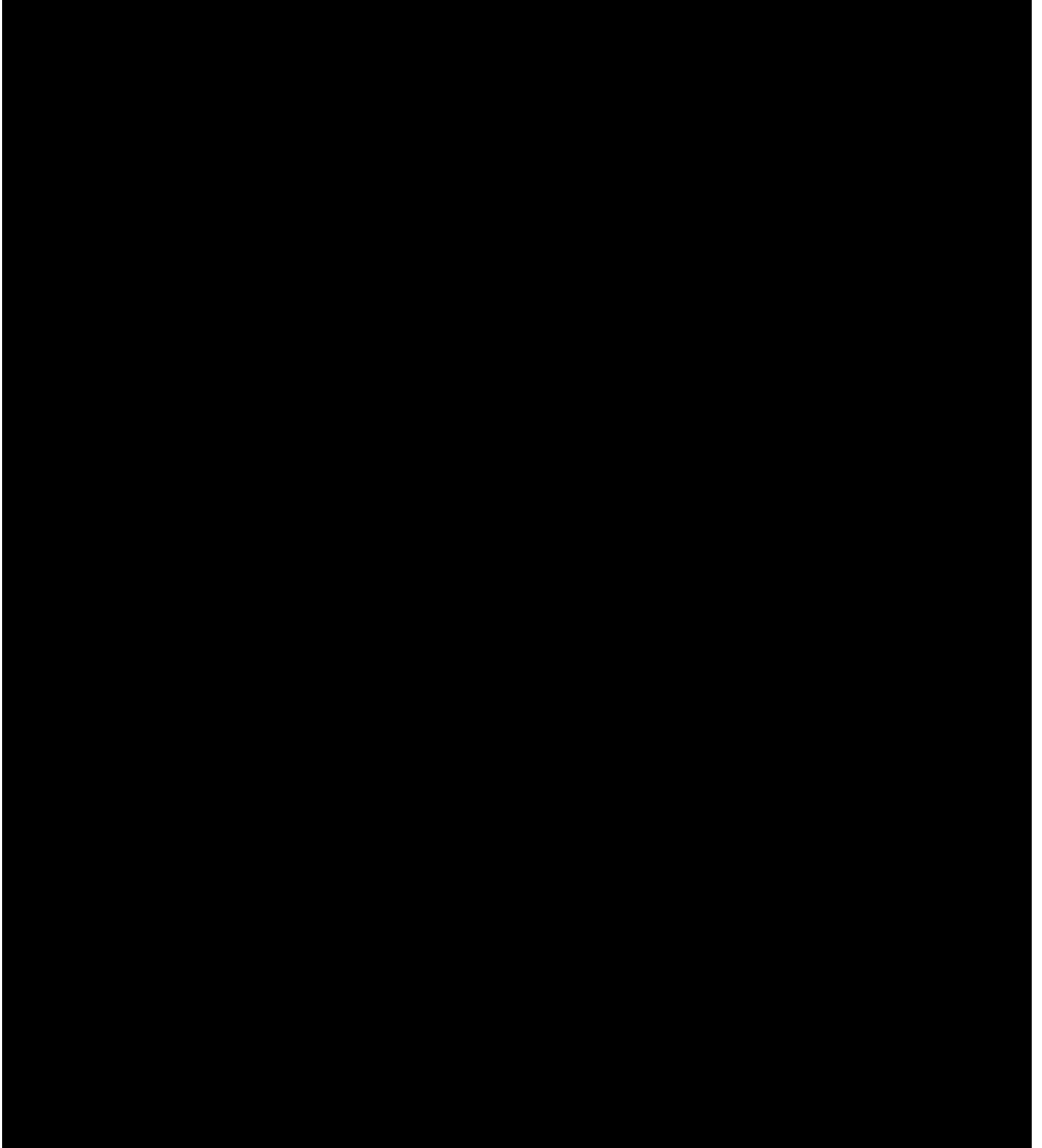
11 Appendix D iCROSS letter of Informed Consent and Participant Information Sheet

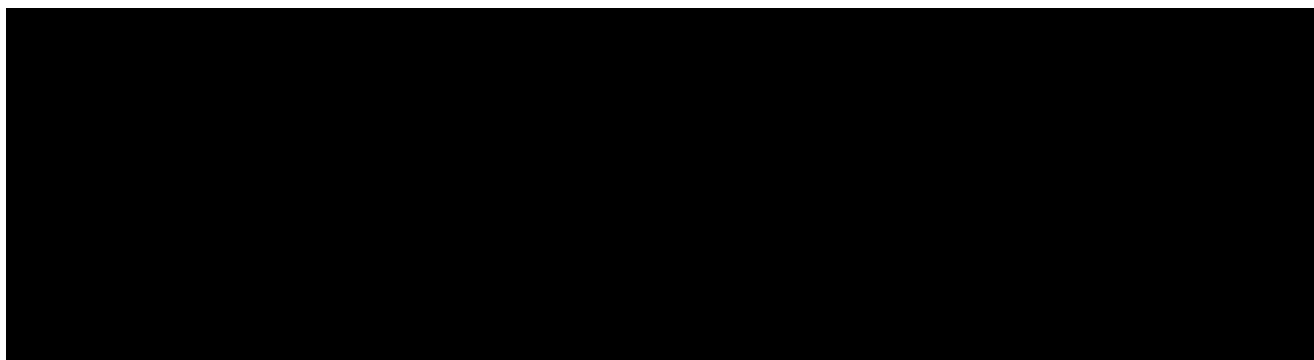




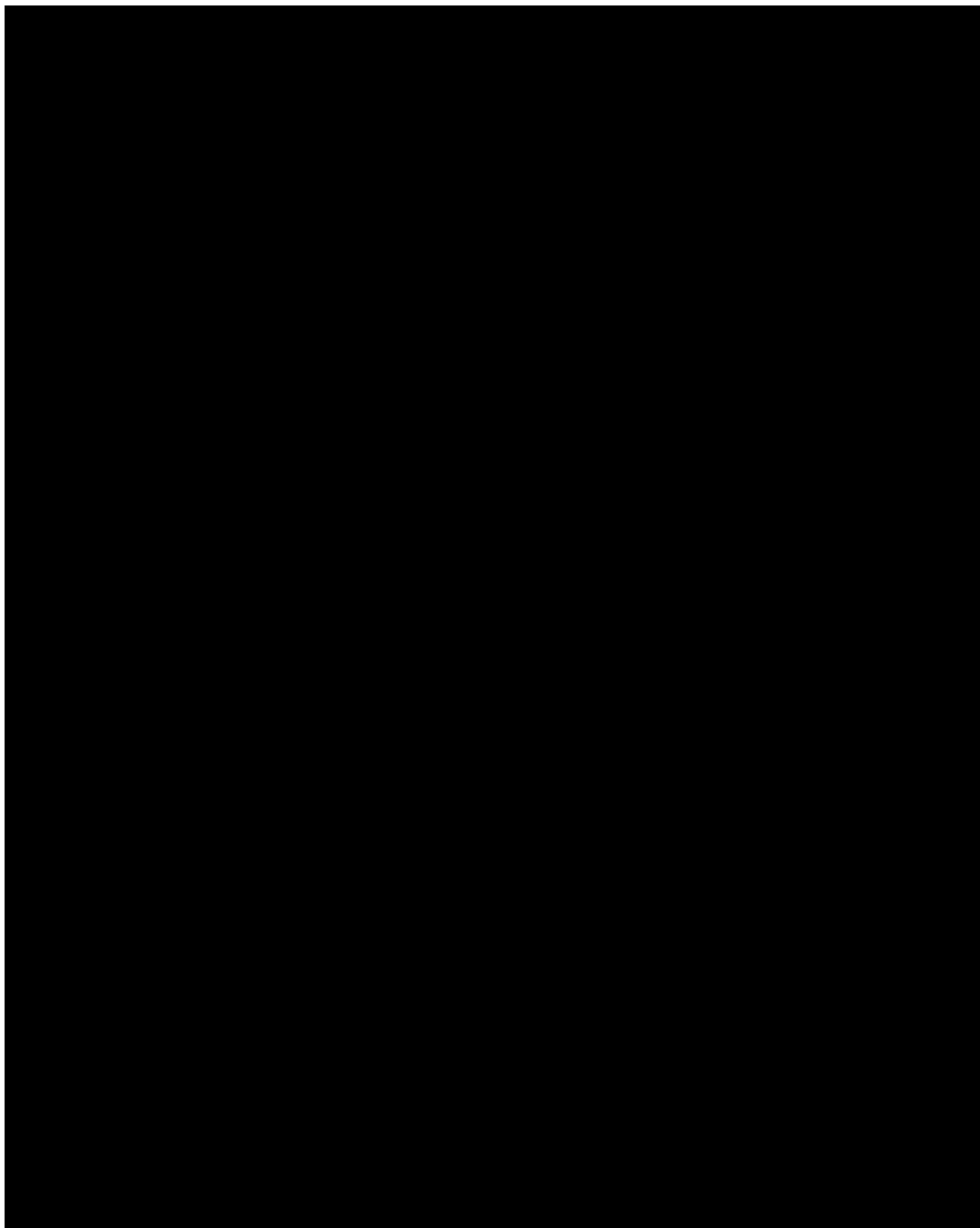
12 Appendix E Border Guard Interview Protocol

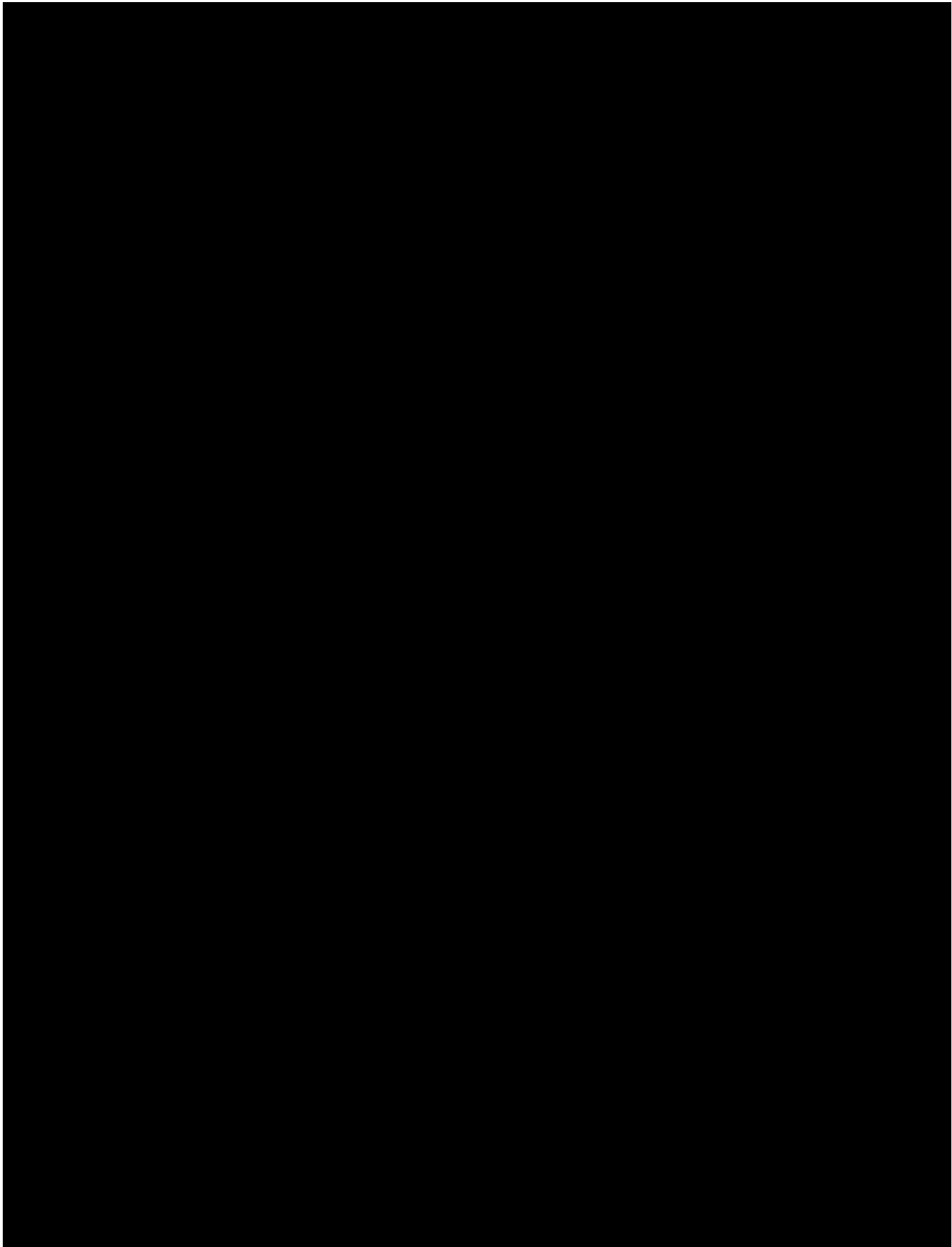
12.1 English Version



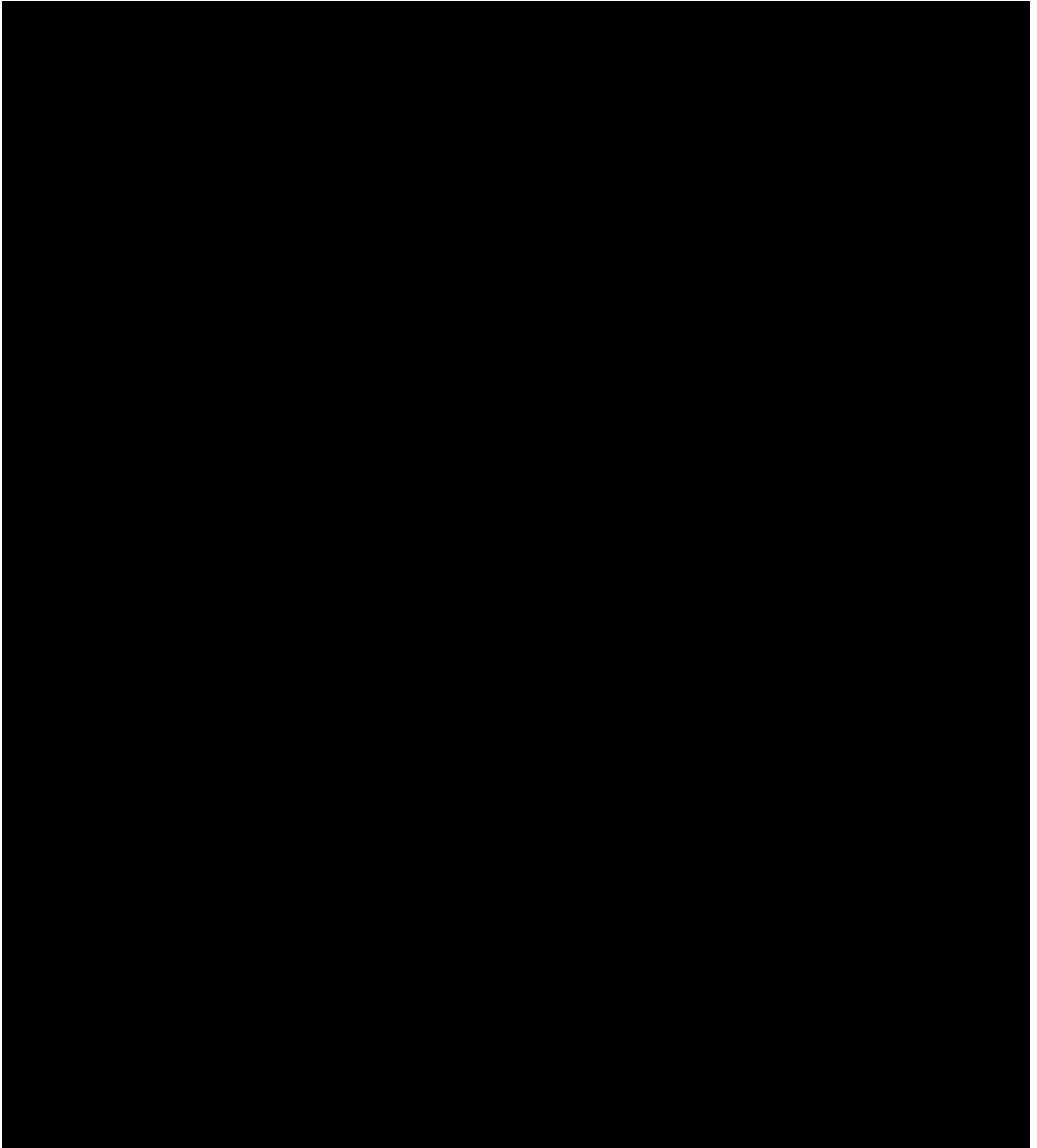


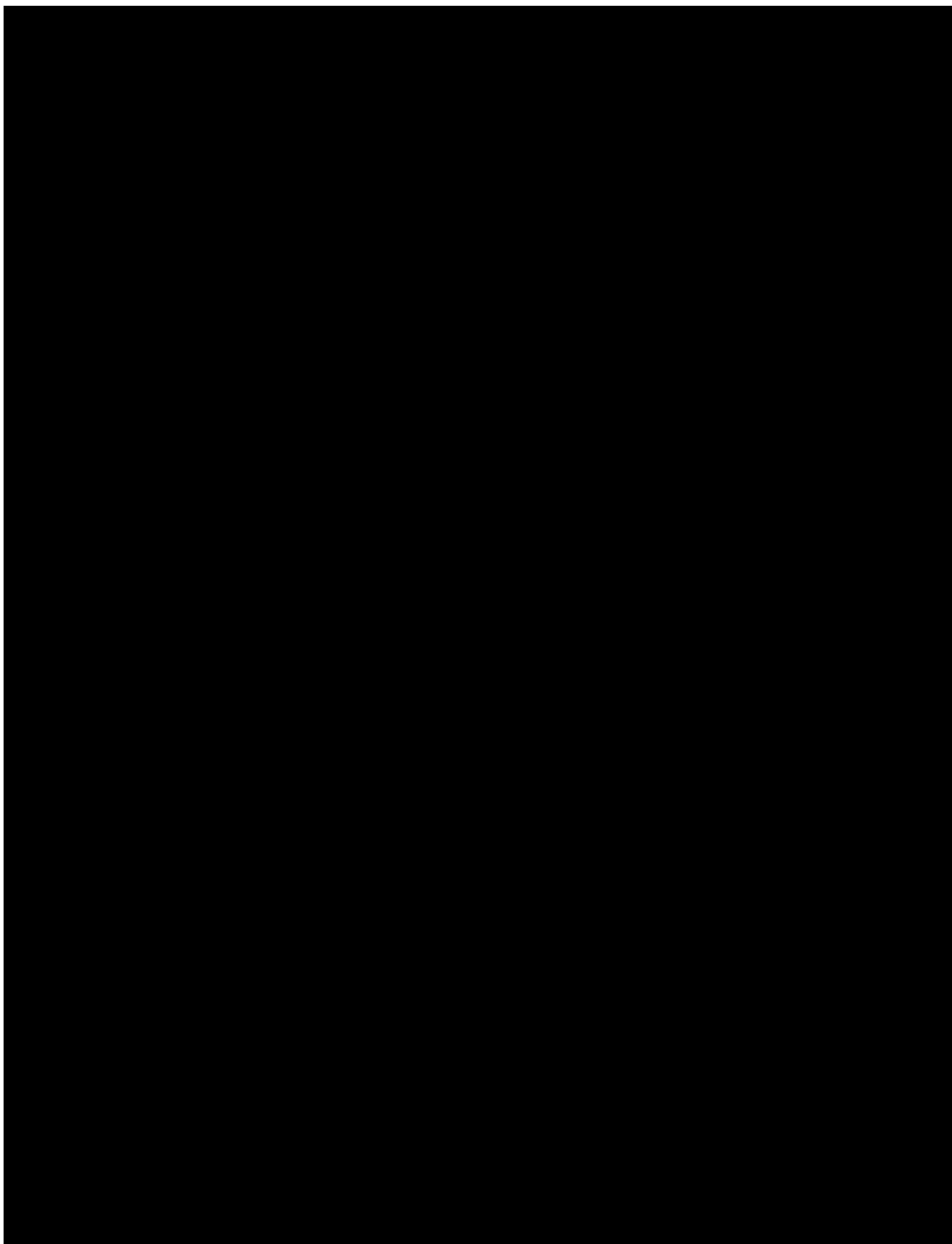
13 Appendix F Border Guard Interview List of Queries

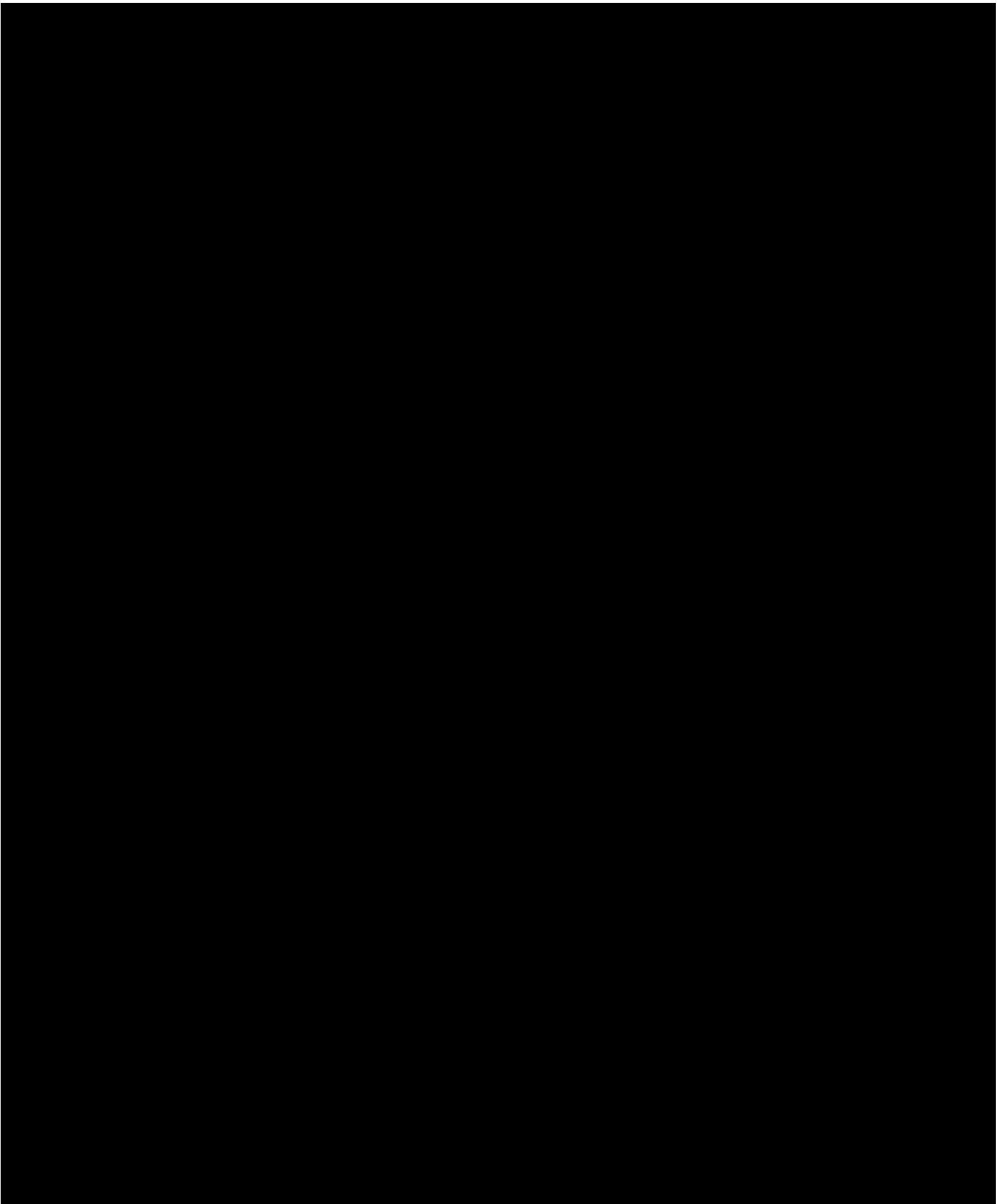


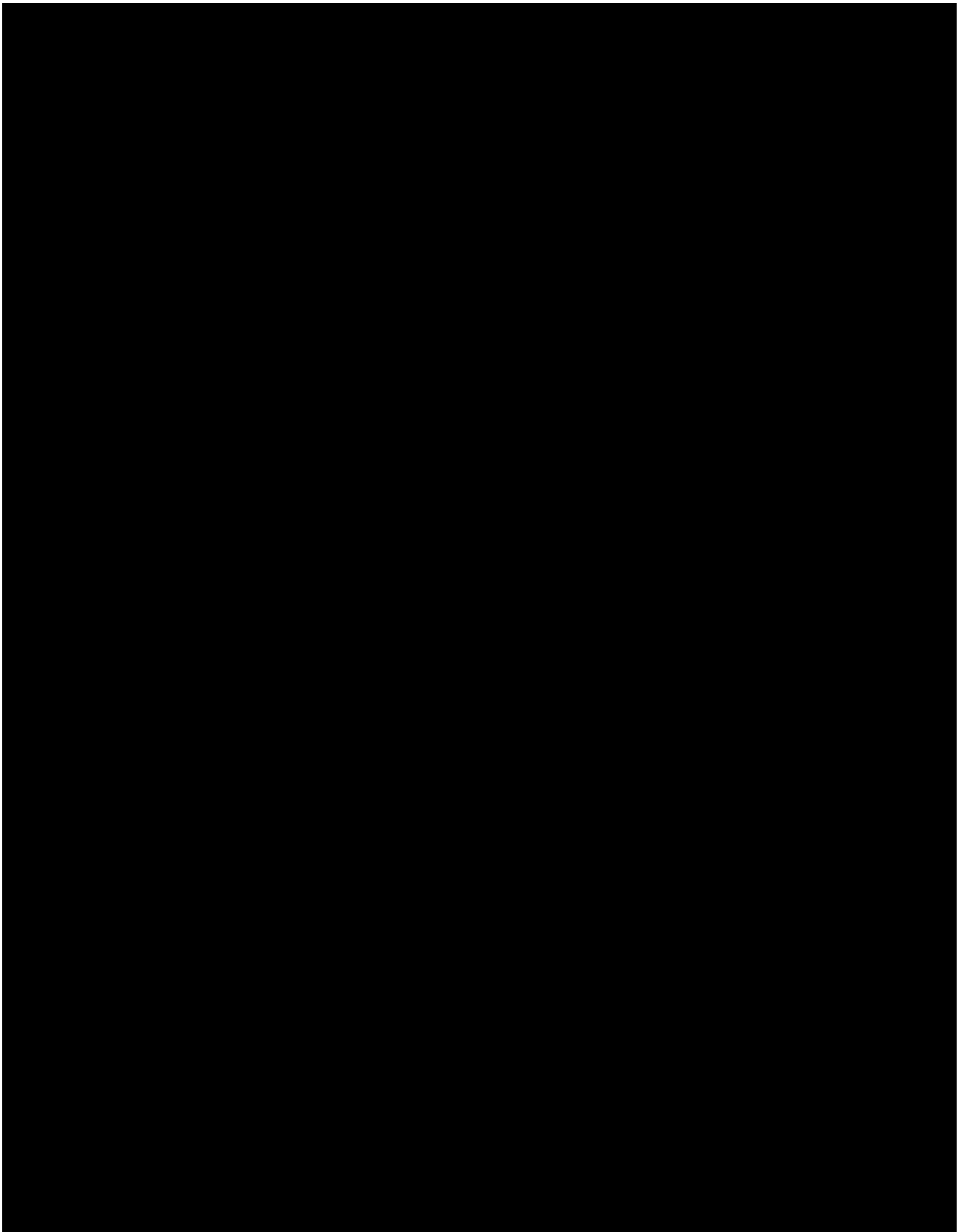


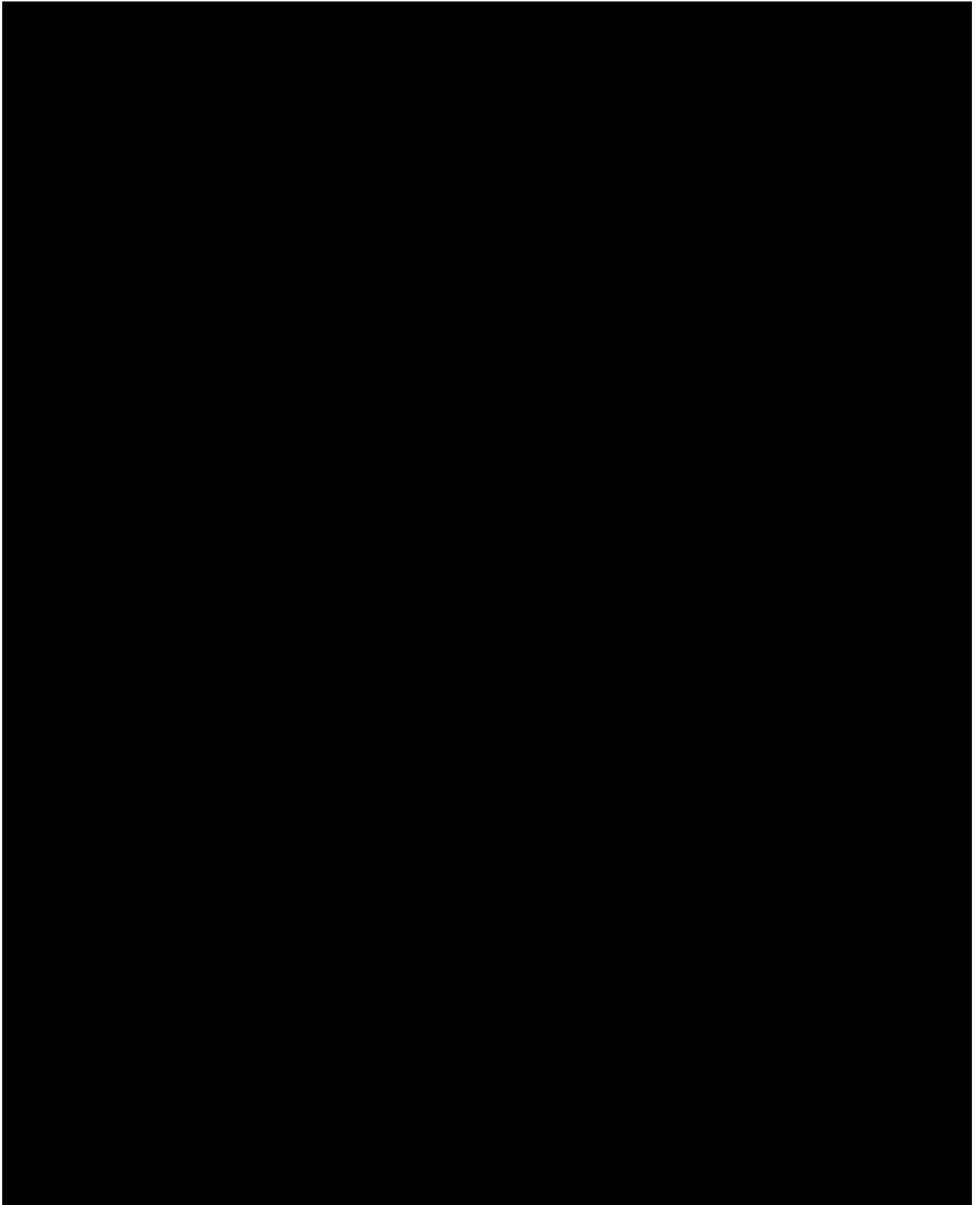
14 Appendix G Results from Travelers Questionnaire

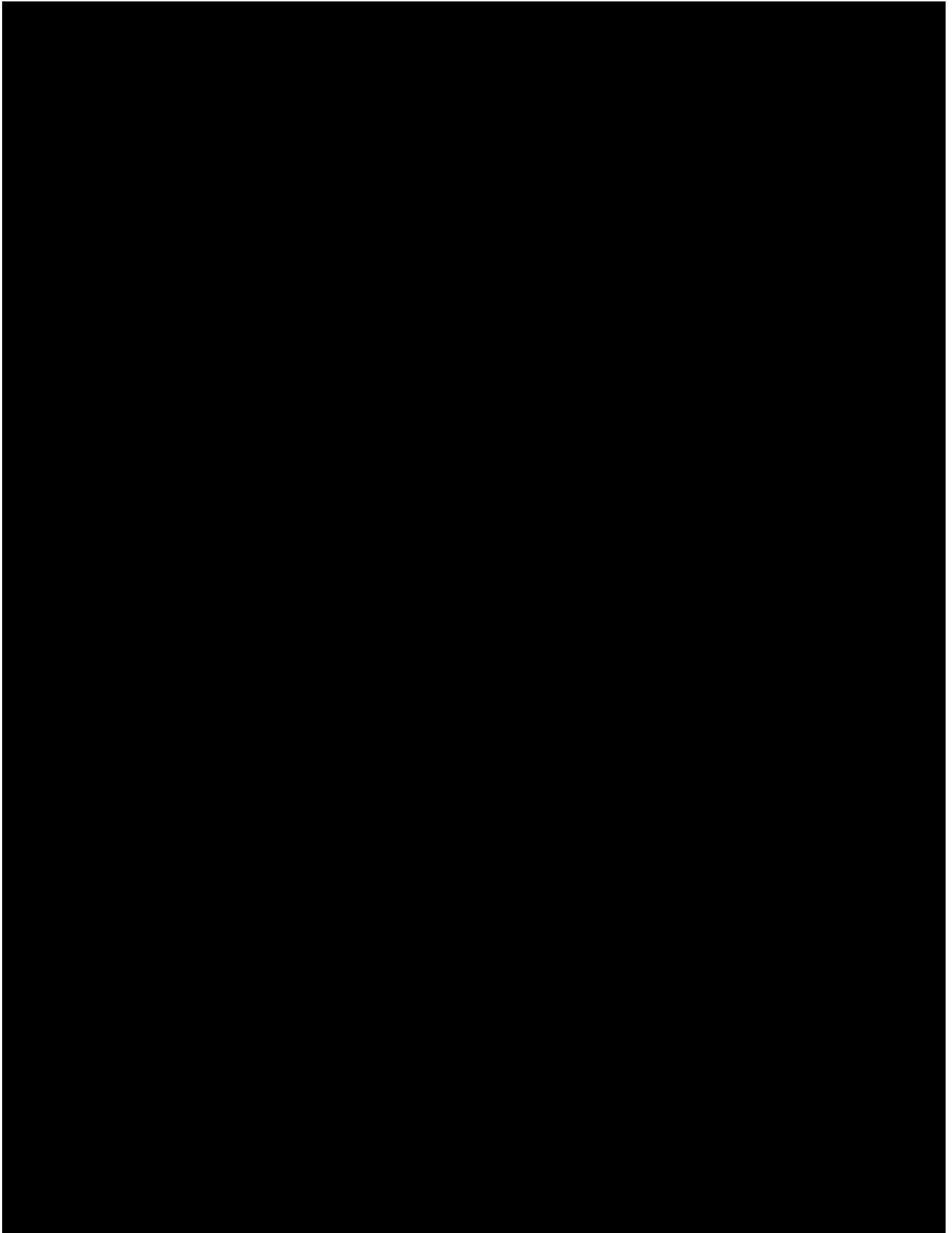


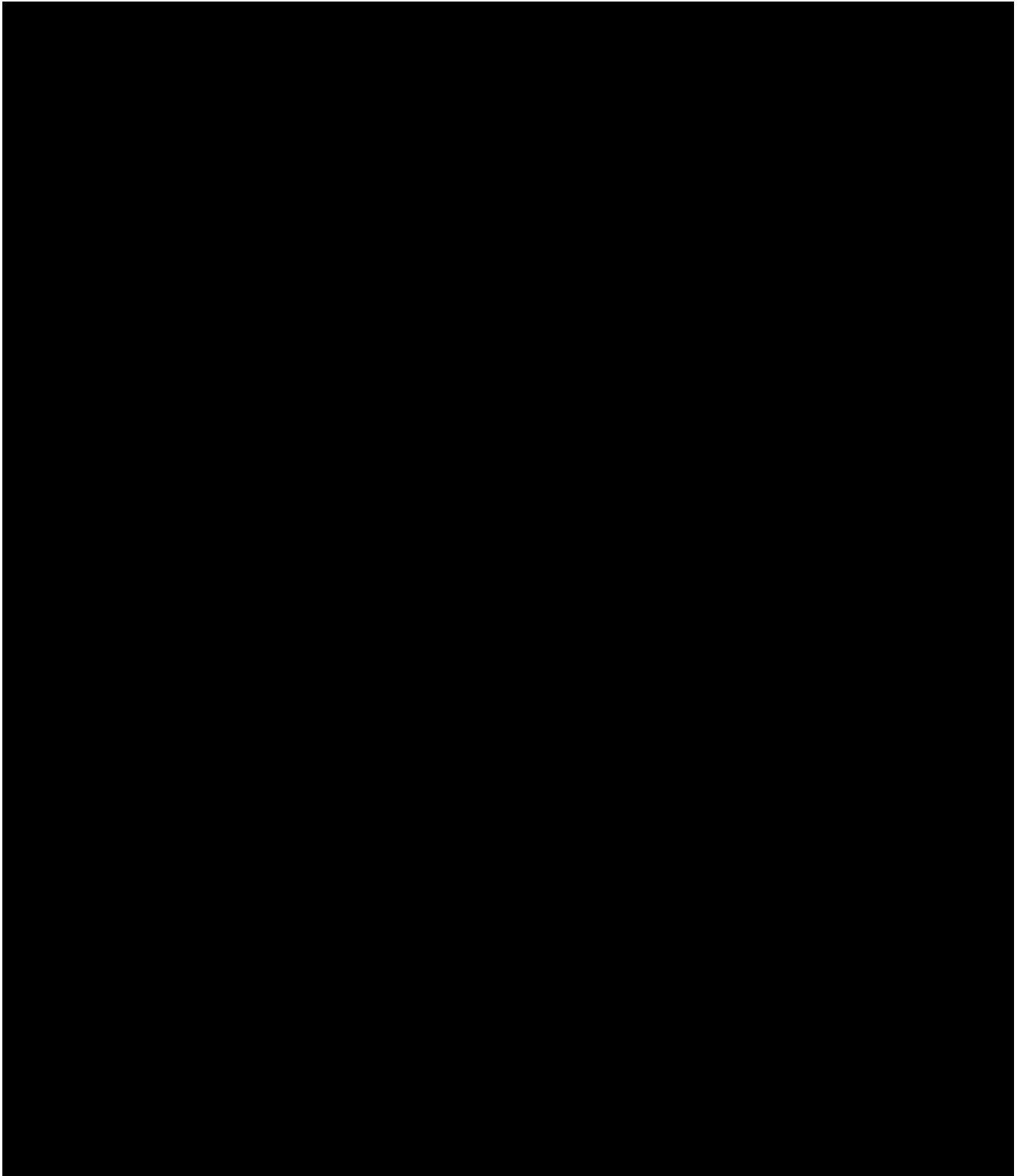


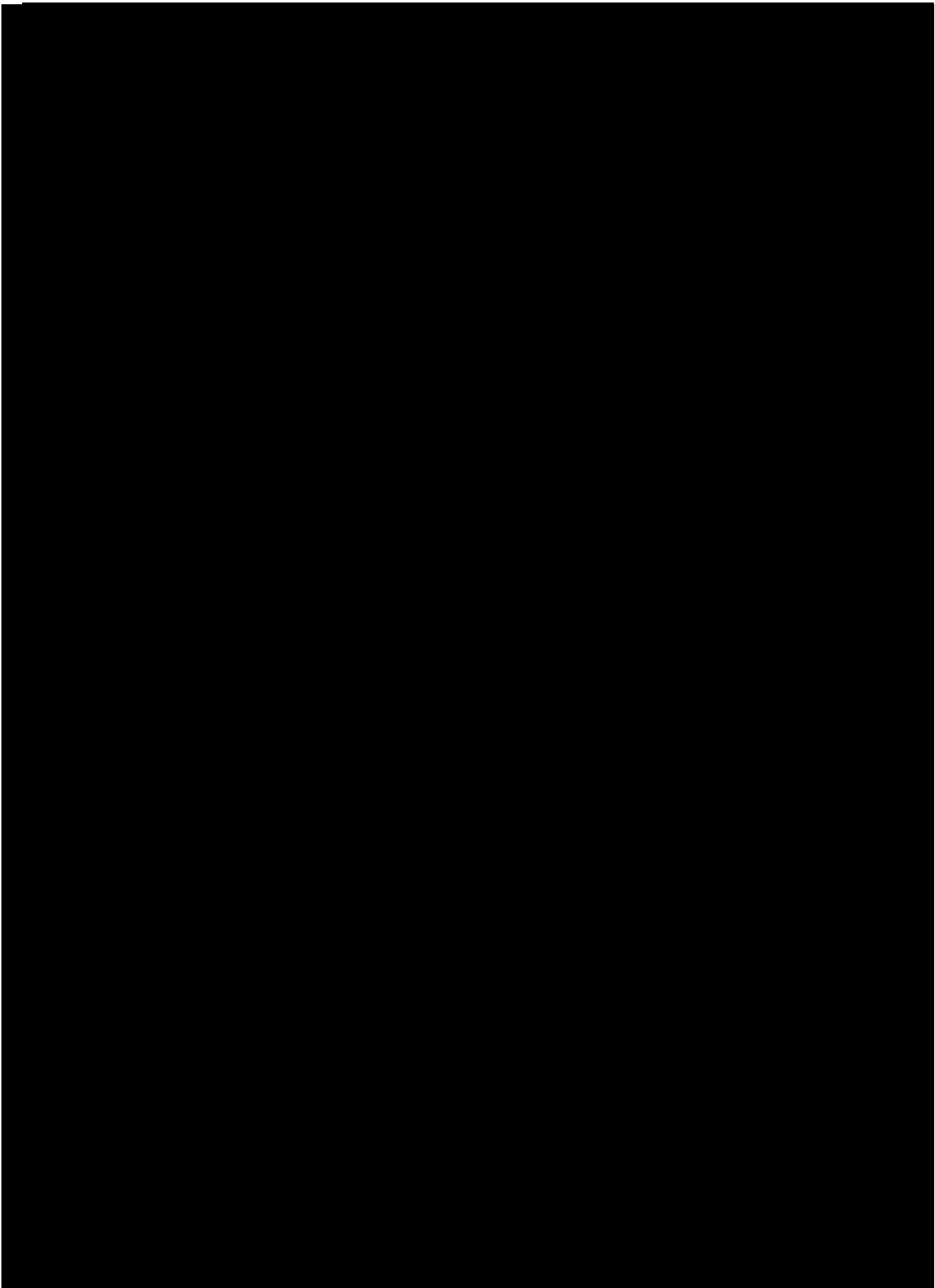


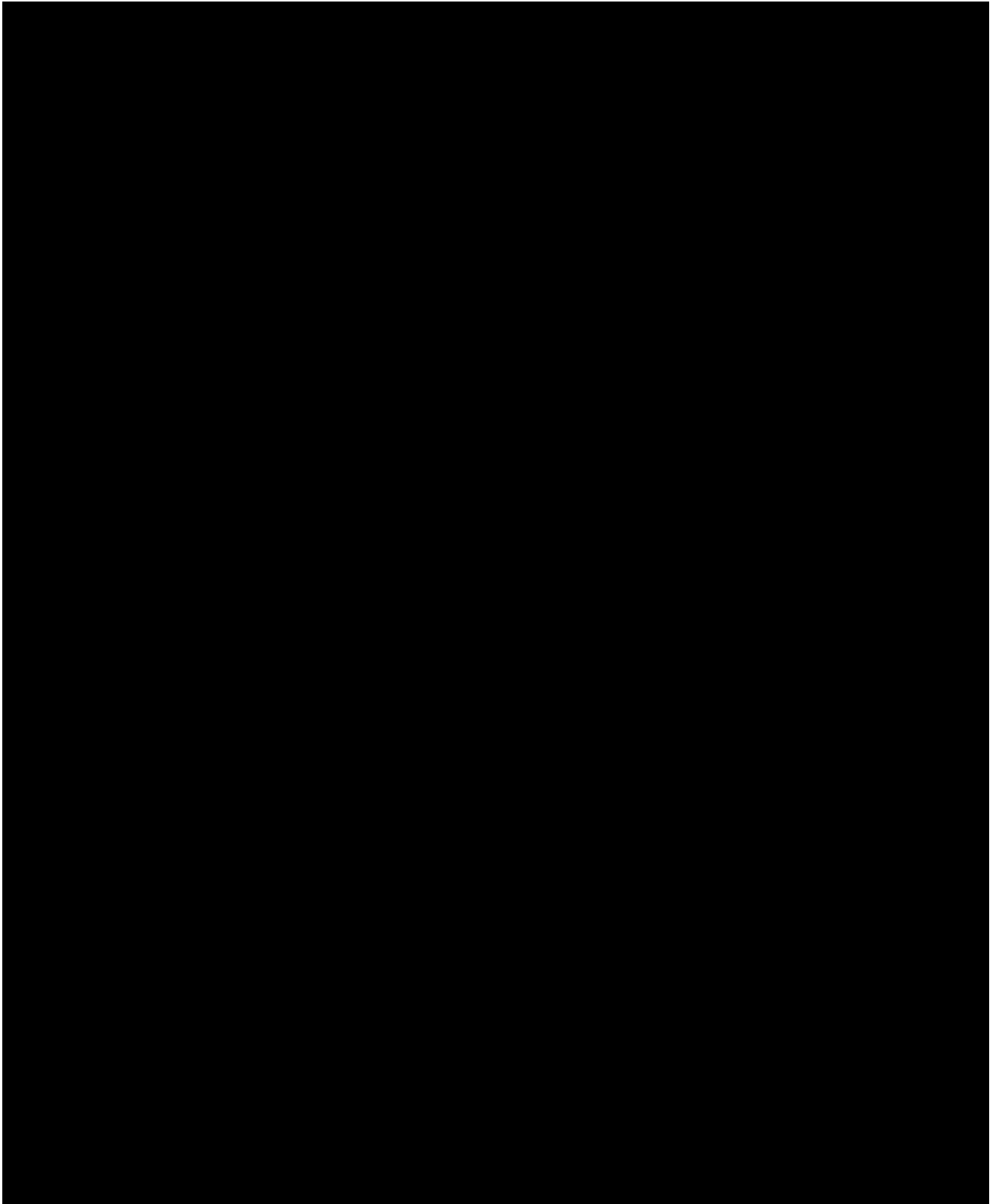


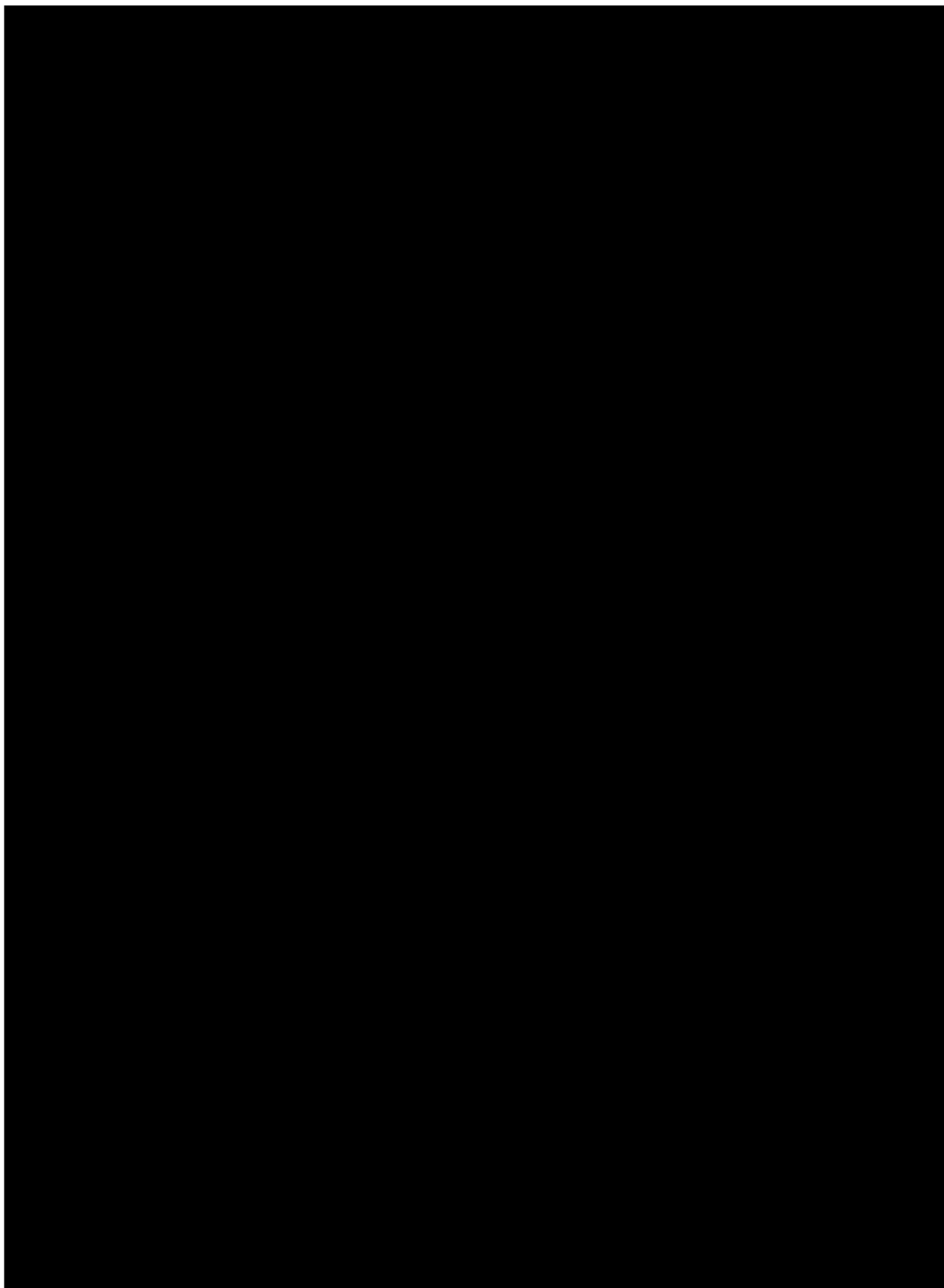


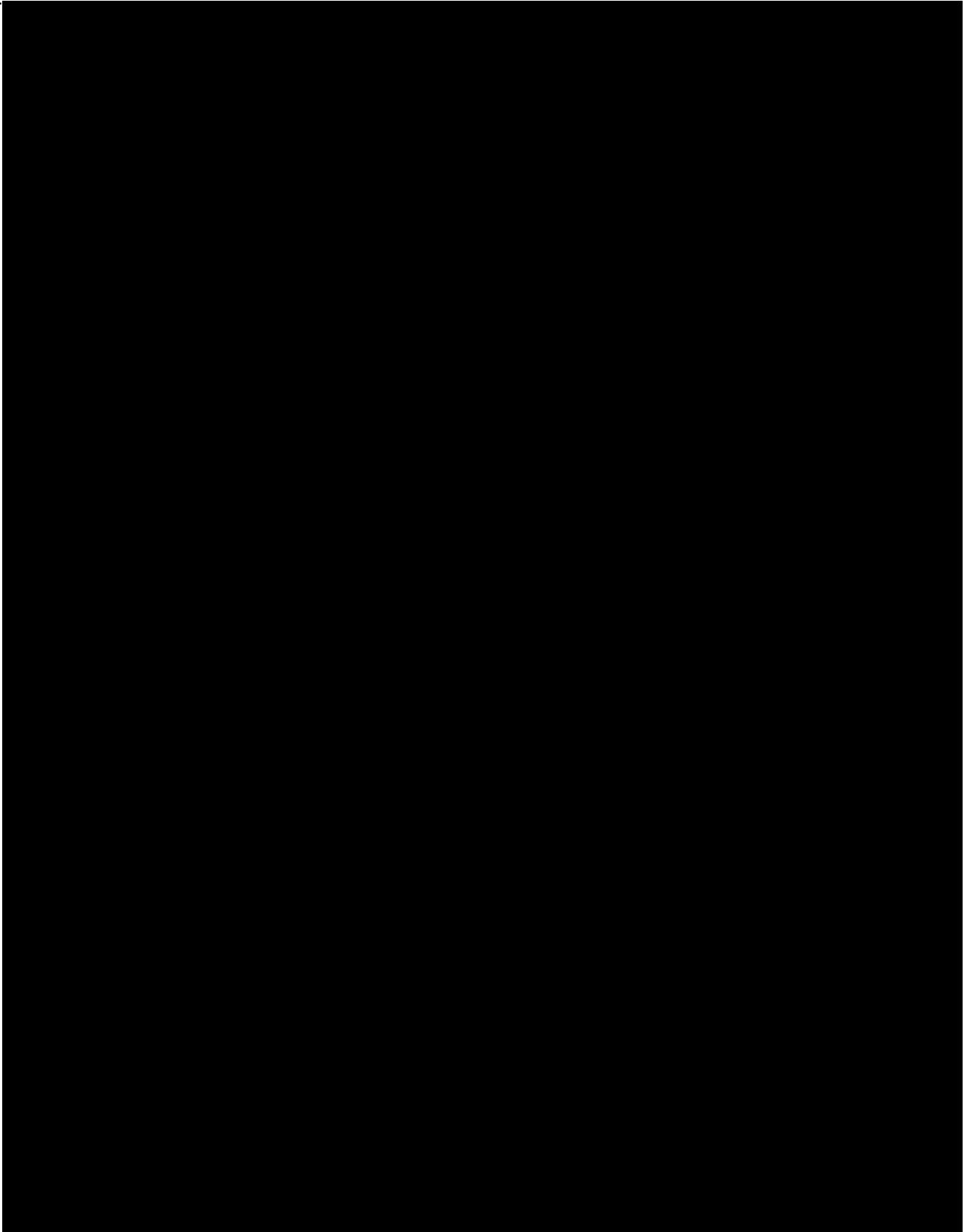


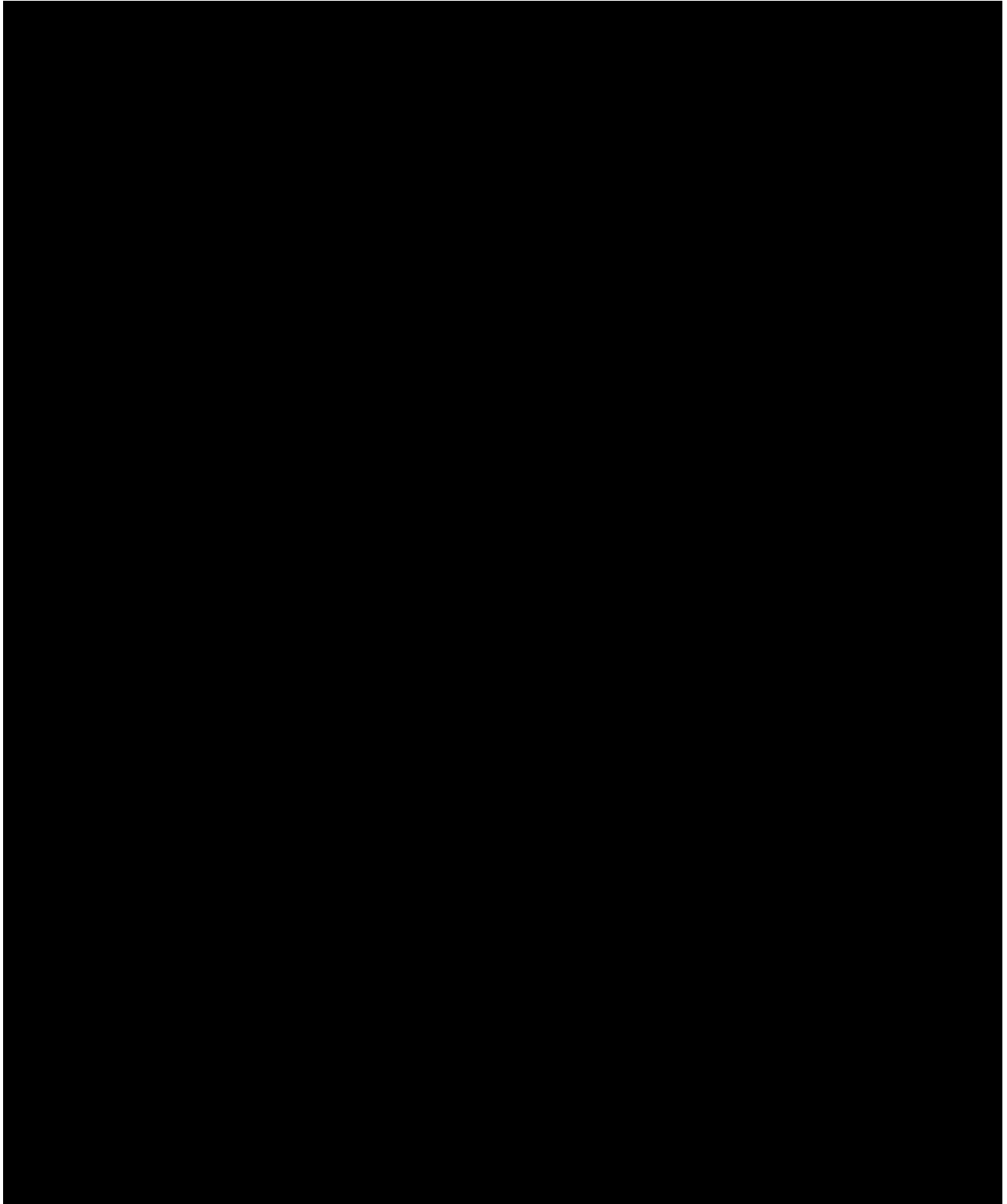


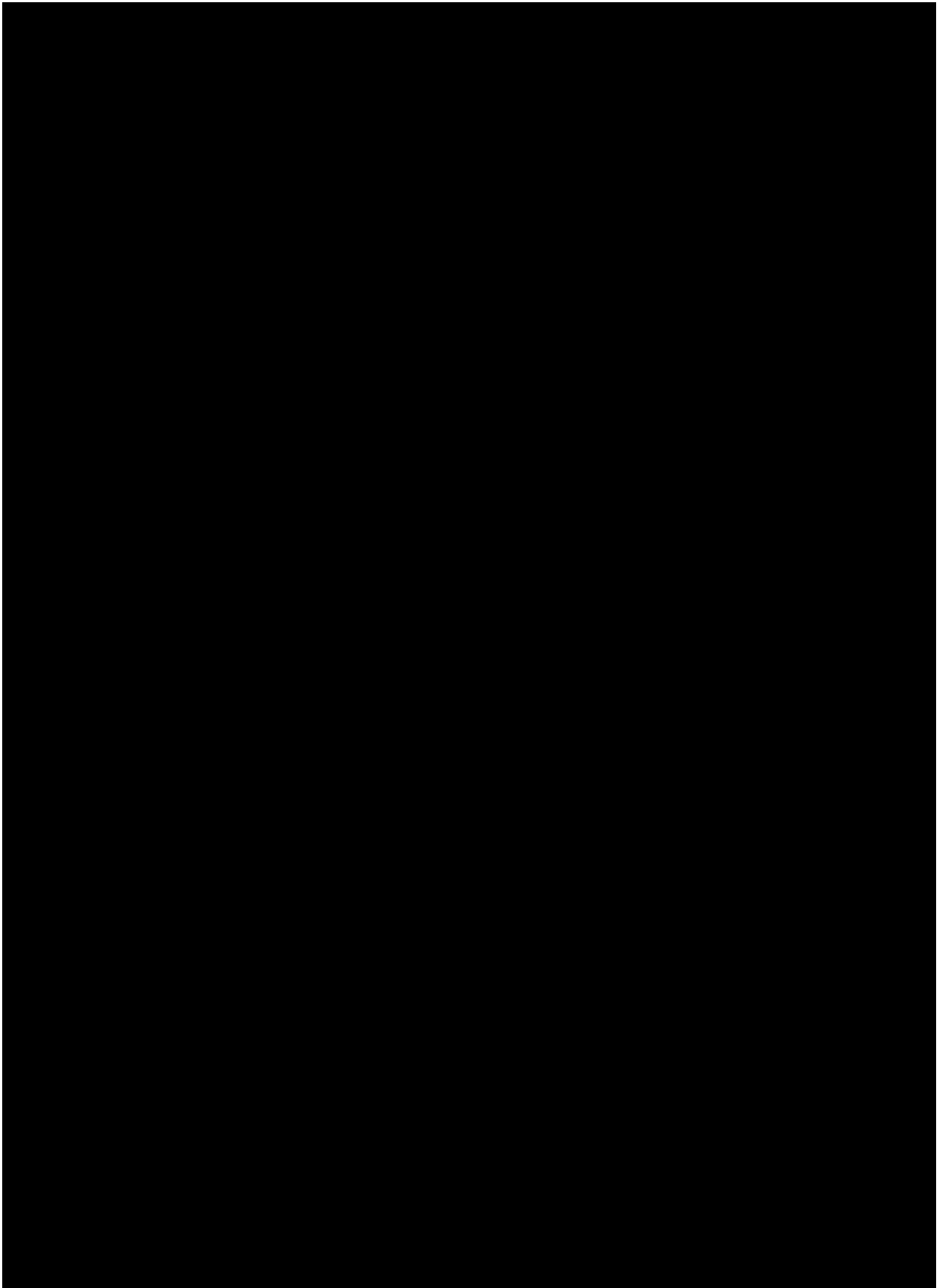


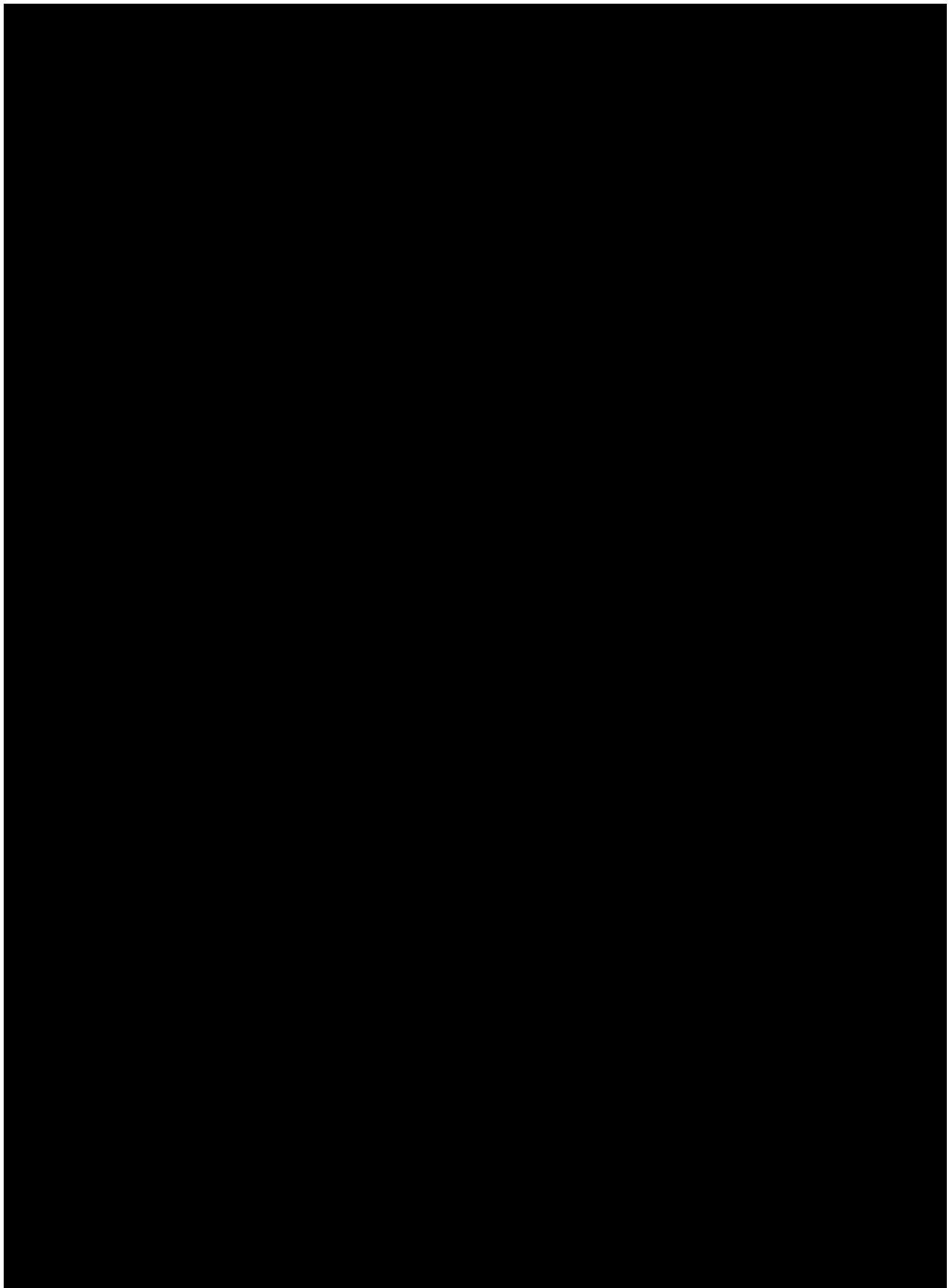


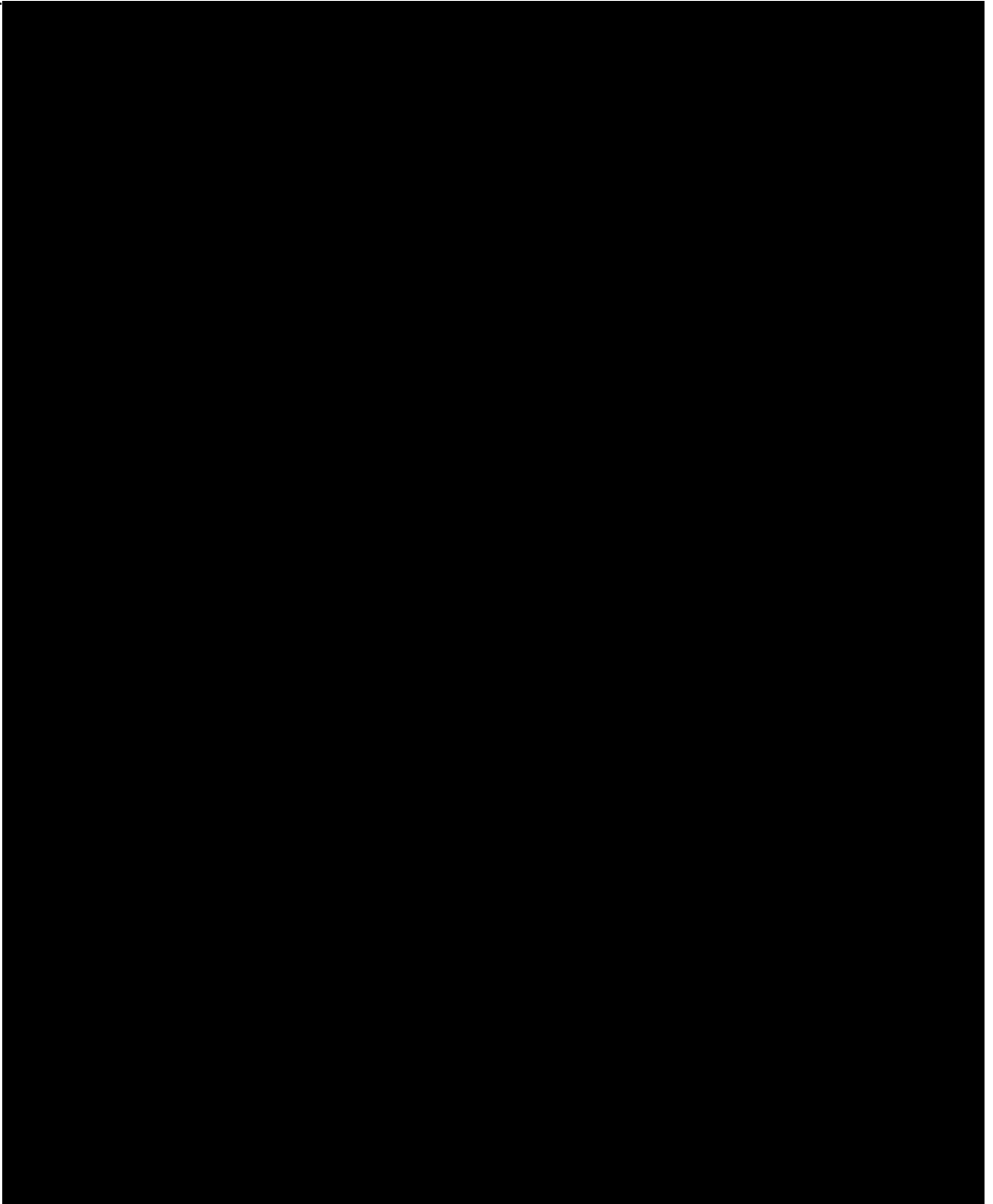


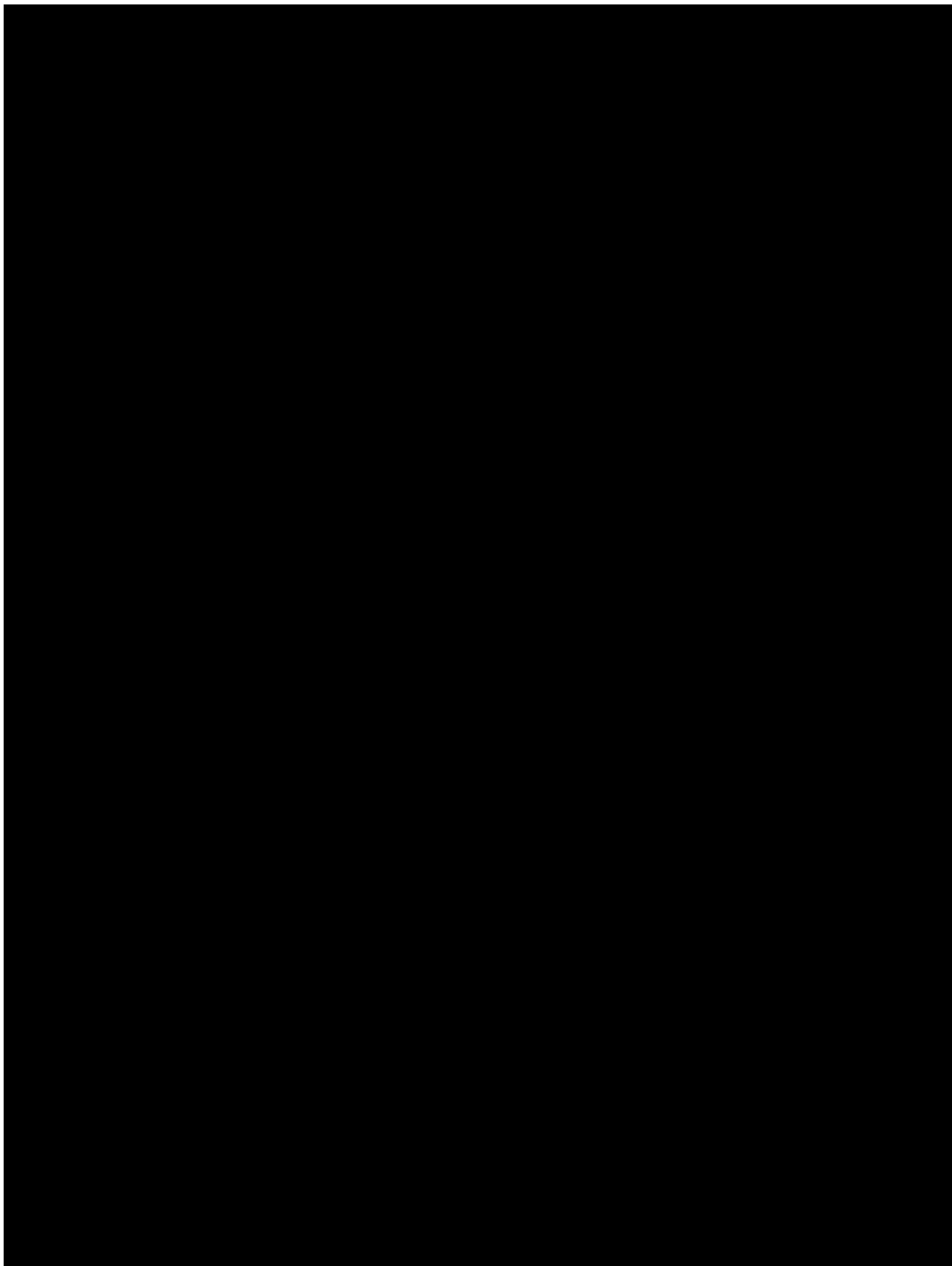


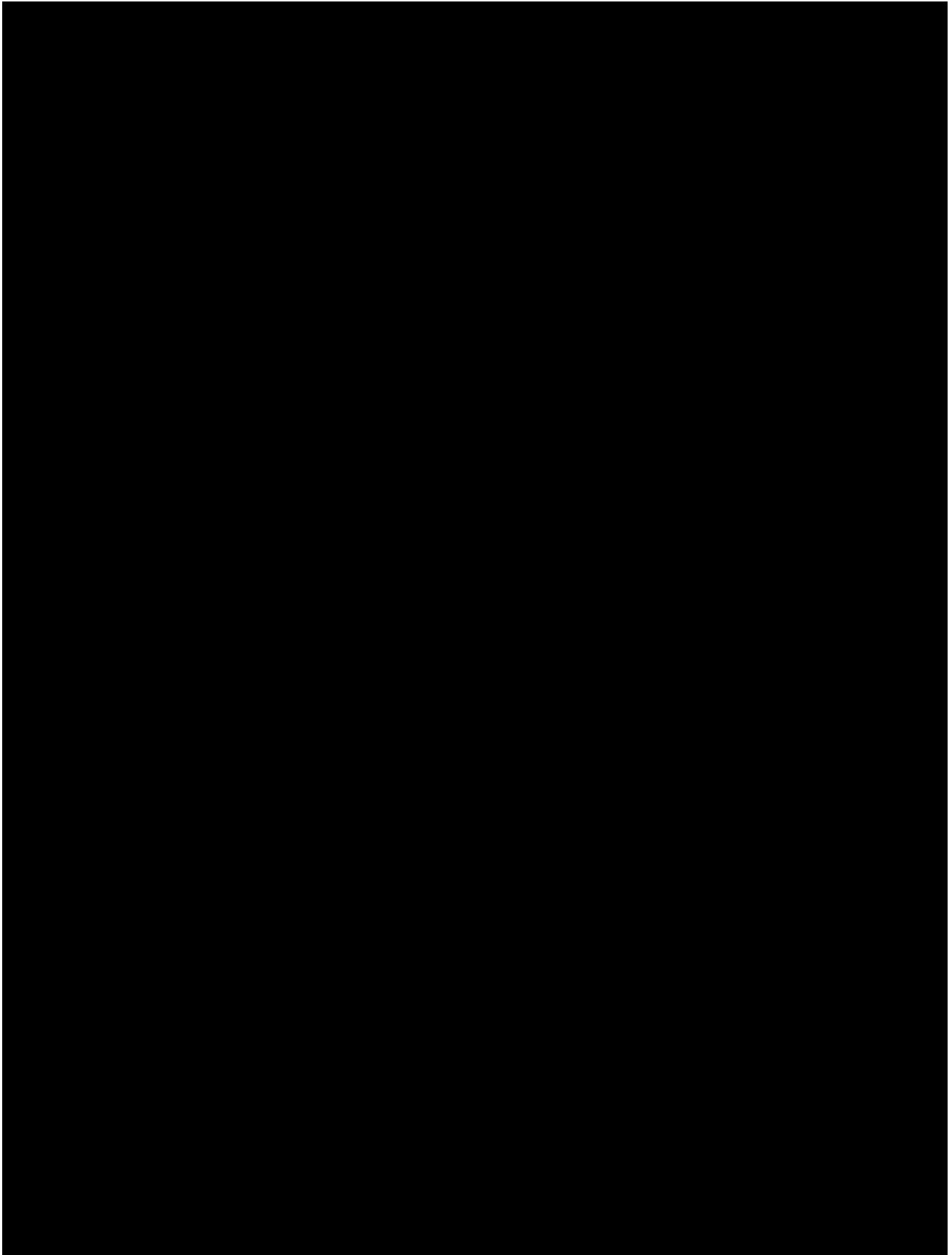


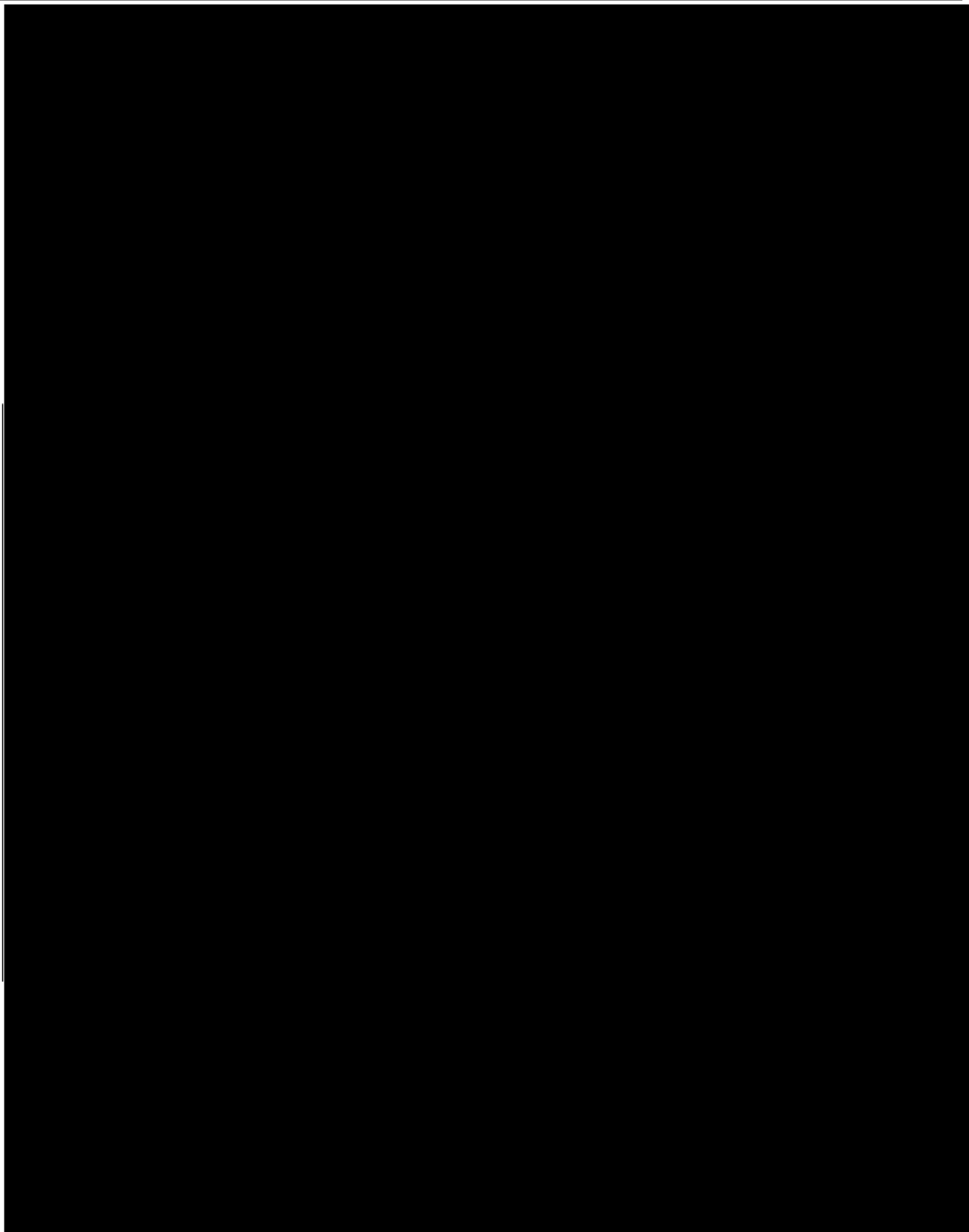


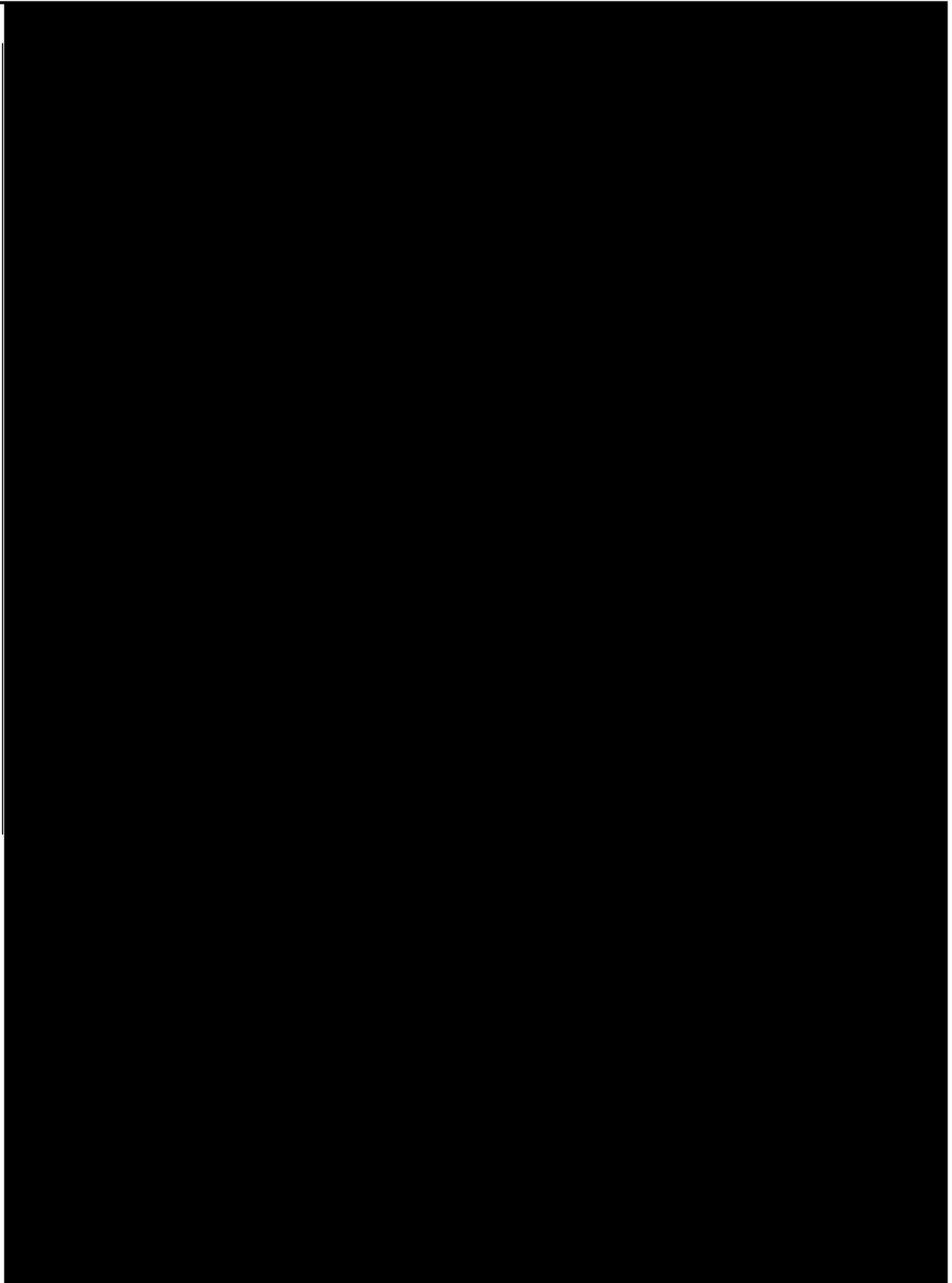


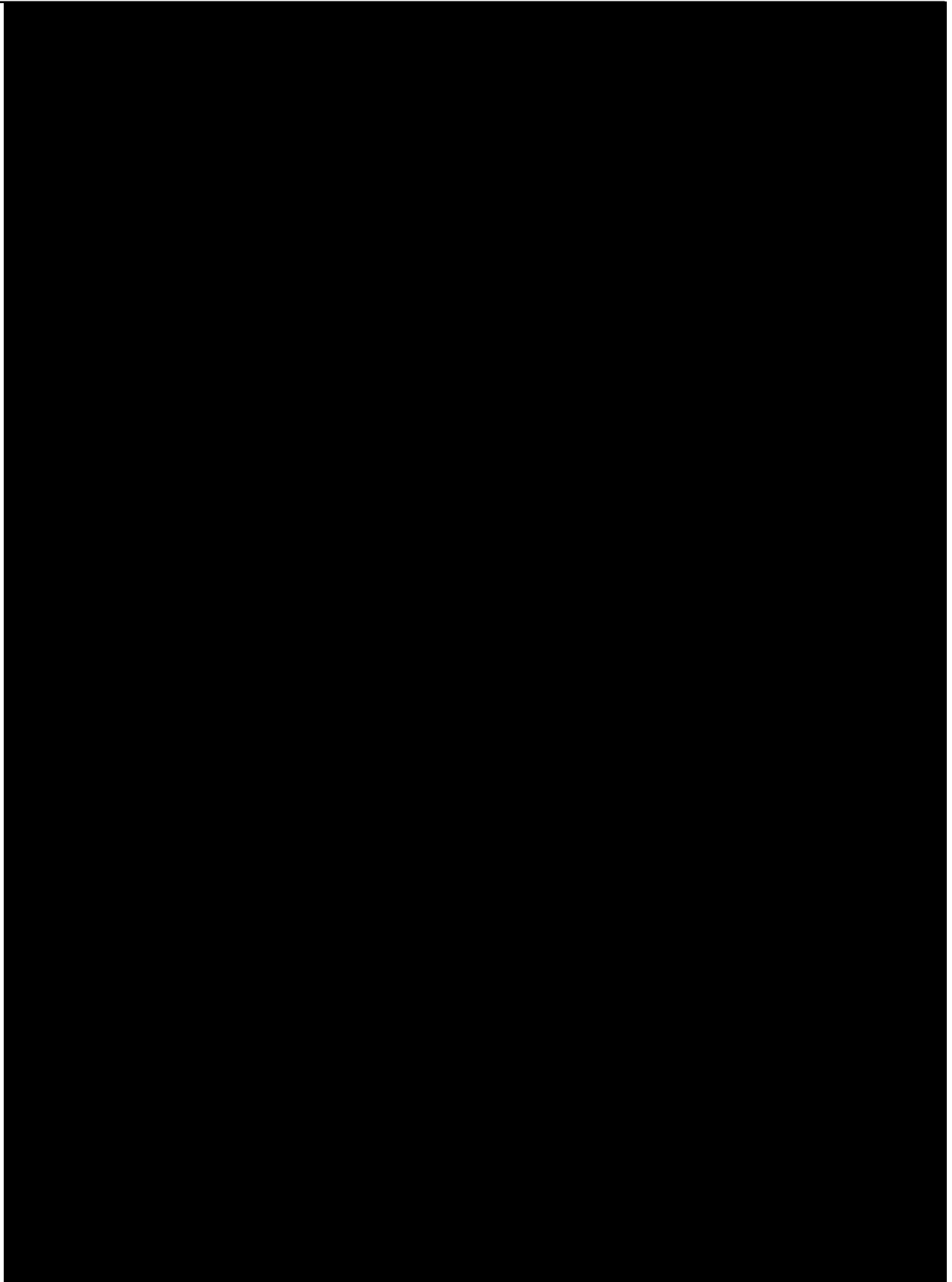


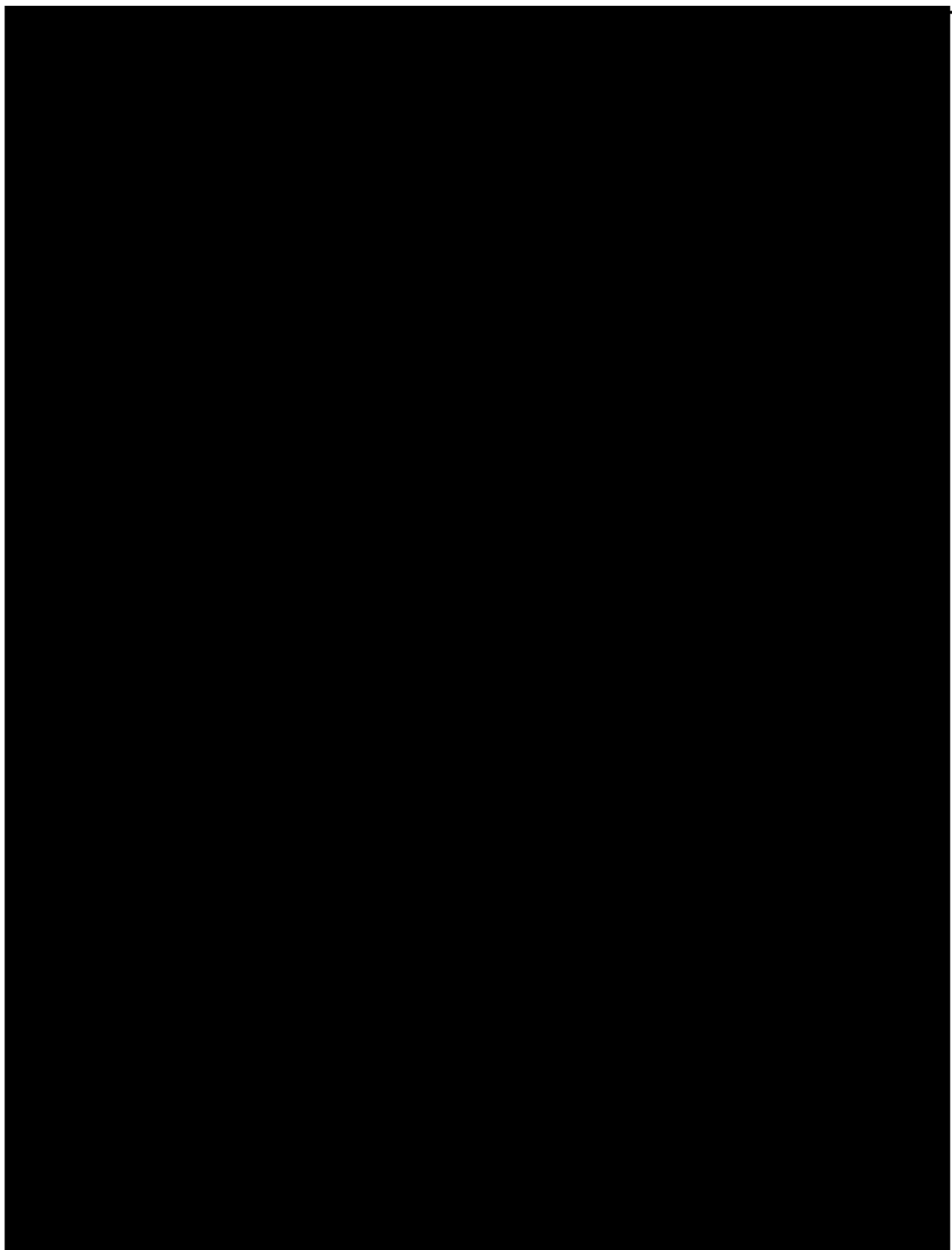


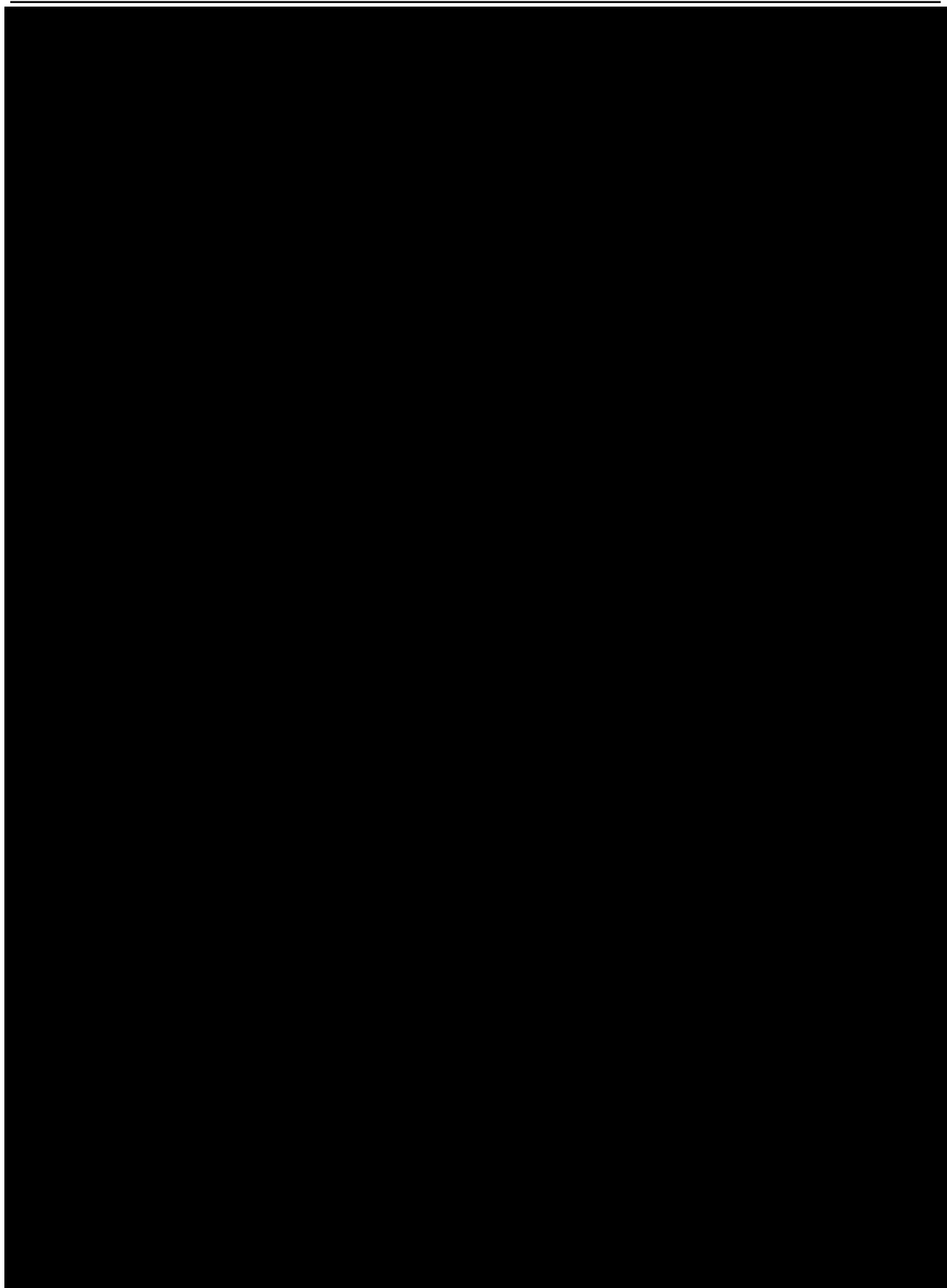


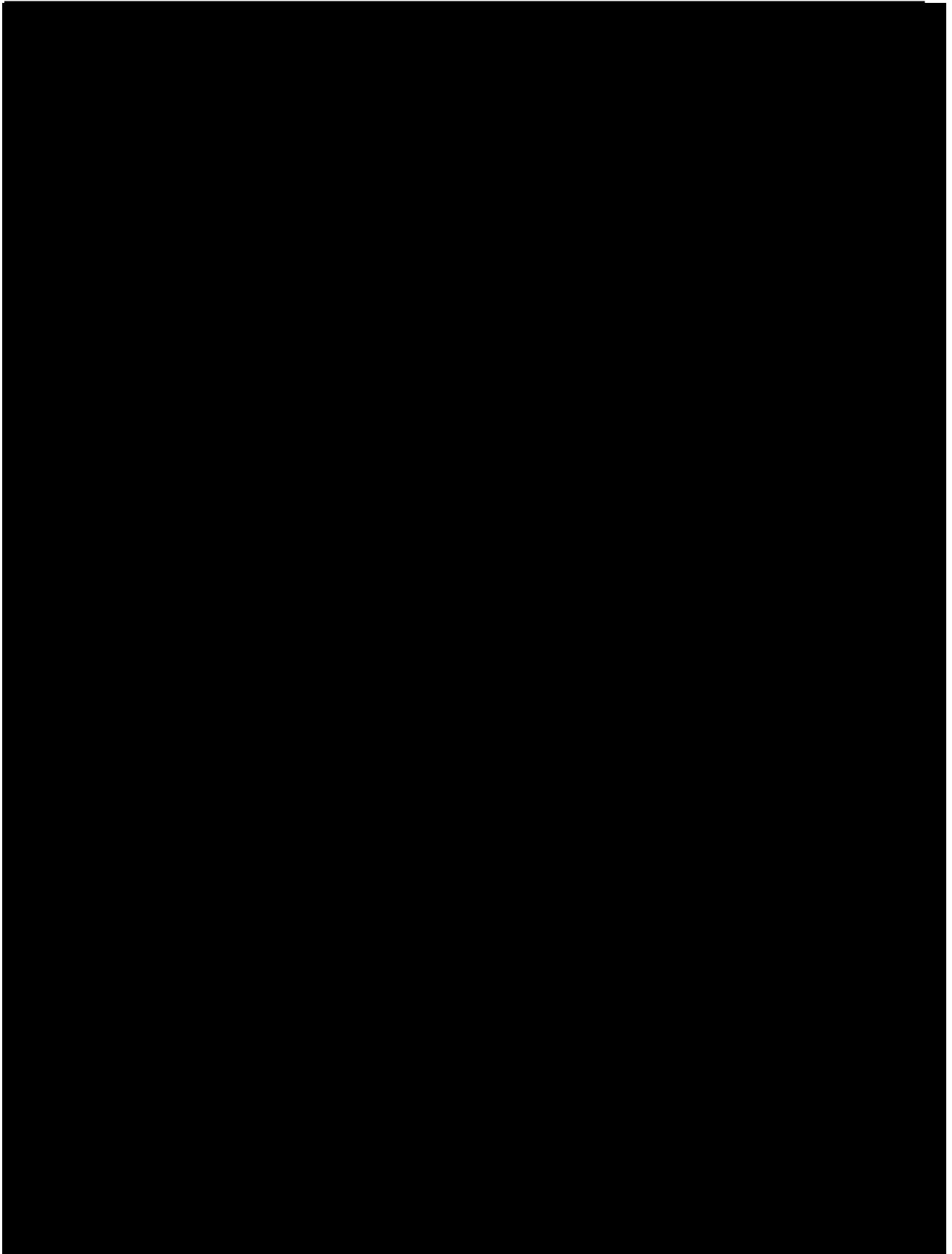












15 Appendix H Statistical Analysis of the Results from the Border Guard / Managers Interviews

