SMLOUVA č. 2201 5 7370

o poskytnutí účelové podpory na řešení programového vývojového projektu

CYBERTHREATS – Využití umělé inteligence při obraně proti kybernetickým útokům

SMLUVNÍ STRANY

1. Česká republika – Ministerstvo obrany

se sídlem:	Tychonova 1, 160 01 Praha 6
jejímž jménem jedná:	JUDr. Pavlína ČERMÁKOVÁ, ředitelka odboru centrálních běžných výdajů Sekce vyzbrojování a akvizic MO
se sídlem kanceláří:	nám. Svobody 471, 160 01 Praha 6
IČO:	60162694
DIČ:	CZ60162694
bankovní spojení:	Česká národní banka, pobočka 701 Na Příkopě 28, 110 03 Praha 1
číslo účtu:	404881/0710

kontaktní osoba ve věcech smluvních (např. zpracování dodatků ke smlouvě):
Ing. Valéria KIŇŠTOVÁ,
[redacted]

kontaktní osoba ve věcech technicko-organizačních (např. účast na oponentních řízeních a kontrolních dnech): Mgr. Pavol CHRENKO,
[redacted]

adresa pro doručování korespondence:
Sekce vyzbrojování a akvizic MO
odbor centrálních běžných výdajů
nám. Svobody 471
160 01 Praha 6

(dále jen „poskytovatel“) na straně jedné

a

2. CESNET, zájmové sdružení právnických osob

zapsán ve spolkovém rejstříku, vedeném Městským soudem v Praze, oddíl L, vložka 58848

se sídlem:	Zikova 1903/4, 160 00 Praha 6
jehož jménem jedná:	Ing. Jakub PAPÍRNÍK, ředitel
IČO:	63839172
DIČ:	CZ63839172
bankovní spojení:	Komerční banka a.s., pobočka Praha 6
číslo účtu:	19-8482200297/0100
kontaktní osoba ve věcech smluvních:	Mgr. Martin Čuřík [redacted]

kontaktní osoba ve věcech technicko-organizačních: [redacted]
adresa pro doručování korespondence: Zikova 1903/4
160 00 Praha 6

(dále jen „příjemce“) na straně druhé,

uzavřely podle § 9 zákona č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o podpoře výzkumu a vývoje“) a v souladu s § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ.“) tuto Smlouvu o poskytnutí podpory na řešení programového projektu (dále jen „Smlouva“).

Článek 1
Účel Smlouvy

Účelem Smlouvy je poskytnutím účelové podpory formou dotace z výdajů na výzkum a vývoj poskytovatele v rámci programu 907 050 (Ambice – podpora rozvoje oblastí, ve kterých ozbrojené složky dosahují významných výsledků v rámci NATO a EU) vyřešit projekt
„**CYBERTHREATS – Využití umělé inteligence při obraně proti kybernetickým útokům**“ (dále jen „projekt“).

Článek 2
Předmět Smlouvy

1. Předmětem Smlouvy je řešení projektu obranného experimentálního vývoje.
2. Výsledkem řešení projektu bude:
    a) prototyp CYBERTHREATS - Využití umělé inteligence při obraně proti kybernetickým útokům;
    b) výrobní dokumentace k prototypu CYBERTHREATS - Využití umělé inteligence při obraně proti kybernetickým útokům.

3. Etapy vývoje, výstupy a termíny řešení projektu:

Etapa č. 1:
- Předběžný projekt prototypu CYBERTHREATS

Výstup: Zápis z oponentního řízení k předběžnému projektu
Termín do 31. 5. 2022

Etapa č. 2:
- Konečný projekt prototypu CYBERTHREATS

Výstup: Zápis z oponentního řízení ke konečnému projektu
Termín do 31. 7. 2022

Etapa č. 3:
- Výrobní dokumentace prototypu CYBERTHREATS

Výstup: Výrobní dokumentace prototypu CYBERTHREATS
Termín do 28. 2. 2023

Etapa č. 4:

- Výroba prototypu CYBERTHREATS

Výstup: Vyrobený prototypu CYBERTHREATS
Termín do 30. 9. 2024

Etapa č. 5:

- Průvodní a provozní dokumentace prototypu CYBERTHREATS

Výstup: Průvodní a provozní dokumentace prototypu CYBERTHREATS
Termín do 29. 2. 2024

Etapa č. 6:

- Podnikové zkoušky, včetně úprav prototypu CYBERTHREATS po podnikových zkouškách

Výstup: Závěrečná zpráva z podnikových zkouškách, upravený prototyp po podnikových zkouškách
Termín do 31. 3. 2025

Etapa č. 7:

- Kontrolní a schvalovací zkoušky, včetně úprav prototypu CYBERTHREATS po kontrolních a schvalovacích zkouškách

Výstup: Závěrečná zpráva po kontrolních a schvalovacích zkouškách, upravený prototyp po kontrolních a schvalovacích zkouškách
Termín do 31. 7. 2025

Etapa č. 8:

- Vojskové zkoušky, včetně úprav prototypu CYBERTHREATS po vojskových zkouškách

Výstup: Závěrečná zpráva po vojskových zkouškách, upravený prototypu po vojskových zkouškách
Termín do 31. 10. 2025

Etapa č. 9:

- Návrh na zavedení prototypu do užívání v rezortu MO

Výstup: Návrh na zavedení prototypu do užívání v rezortu MO
Termín do 31. 12. 2025

Etapa č. 10:

- Závěrečné oponentní řízení do 60 dnů po ukončení řešení projektu

Výstup: Zápis z oponentního řízení k závěrečné zprávě
Termín do 28. 2. 2026

Etapa č. 11:

- Odevzdání výsledků vývoje do 30 dnů po závěrečném oponentním řízení

Výstup: Protokol o odevzdání výsledků vývoje
Termín do 31. 3. 2026

4. Forma a místo předání výsledků řešení projektu bude stanovena v rámci závěrečného oponentního řízení.
5. Projekt bude realizován v souladu s podmínkami stanovenými touto Smlouvou a jednotlivými přílohami.

Článek 3
Uznané náklady a poskytnutá podpora

1. Uznané náklady projektu jsou stanoveny ve výši **37 776 239 Kč** (slovy: Třicet sedm milionů sedm set sedmdesát šest tisíc dvě stě třicet devět korun českých).
2. Celková výše podpory poskytovatele na projekt činí výši **37 776 239 Kč** (slovy: Třicet sedm milionů sedm set sedmdesát šest tisíc dvě stě třicet devět korun českých).
3. Rozdělení podpory pro příjemce na kalendářní roky:

(hodnoty uvedeny v Kč)

Číslo projektu	Příjemce	Náklady	2022	2023	2024	2025	Celkem
907 050 7370	CESNET	investiční	0	0	0	0	**0**
		neinvestiční	8 034 785	13 247 943	11 390 078	5 103 433	**37 776 239**
Celkem účelová podpora			8 034 785	13 247 943	11 390 078	5 103 433	**37 776 239**
Celkem uznané náklady			8 034 785	13 247 943	11 390 078	5 103 433	**37 776 239**

Článek 4
Trvání Smlouvy a místo plnění

1. Řešení projektu bude zahájeno nejpozději do 60 kalendářních dnů ode dne nabytí účinnosti Smlouvy a ukončeno nejpozději do 31. prosince 2025. Období hodnocení výsledků a vypořádání Smlouvy se stanovuje od 1. ledna 2026 do 30. června 2026.
2. Místem plnění je sídlo příjemce.
3. Místem předání všech zpráv, informací a výkazů čerpání poskytnuté podpory je sídlo poskytovatele.

Článek 5
Řešitel projektu

Osobou odpovědnou příjemci za odbornou úroveň projektu – řešitelem projektu dle § 9 odst. 1 písm. e) zákona o podpoře výzkumu a vývoje je:

[redacted]

Článek 6
Právní vztahy

Vztahy touto smlouvou neupravené se řídí zákonem o podpoře výzkumu a vývoje a OZ.

Článek 7
Zástupci stran a kontaktní osoby

1. Jménem poskytovatele mohou činit právní úkony ve všech záležitostech týkajících se této Smlouvy pouze osoby, oprávněné jednat jménem poskytovatele, uvedené v záhlaví této Smlouvy a jménem příjemce může činit právní úkony ve všech záležitostech, týkajících se této Smlouvy pouze osoba, oprávněná jednat jménem příjemce, uvedená v záhlaví této Smlouvy.

2. Kontaktní osoby smluvních stran, uvedené v záhlaví této Smlouvy, budou zabezpečovat vzájemnou komunikaci, koordinaci, informovanost stran včetně přípravy návrhů příslušných dokumentů. Tyto osoby nejsou oprávněny činit žádné právní úkony.
3. Dojde-li k jakékoli změně osob této Smlouvy, jsou poskytovatel nebo příjemce povinni neprodleně oznámit písemně takovou změnu druhé smluvní straně a taková změna musí být doložena příslušným dokumentem nebo zdůvodněním.

Článek 8
Změny Smlouvy

Smlouva může být měněna pouze vzájemně odsouhlasenými, písemnými, vzestupně číslovanými dodatky ke Smlouvě.

Článek 9
Závěrečná ustanovení

1. Ustanovení Smlouvy mají přednost před ustanoveními přílohy č. 2 Smlouvy.
2. Tato Smlouva nabývá platnosti dnem jejího podpisu druhou ze smluvních stran a účinnosti dnem zveřejnění v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.
3. Smlouva je vyhotovena v elektronické podobě o 5 stranách a 5 přílohách o 58 stranách.
4. Změna identifikačních údajů smluvních stran uvedených v záhlaví této Smlouvy, změna čísel telefonů a faxů uváděných v jednotlivých ustanoveních této Smlouvy, nebude považována za změnu této Smlouvy. Každou změnu podle tohoto článku oznámí příslušná smluvní strana písemně druhé straně neprodleně poté, co se o ní dozvěděla.
5. Nedílnou součástí Smlouvy jsou následující přílohy:

příloha č. 1 – Všeobecné podmínky ke smlouvě	počet stran: 9
příloha č. 2 – Návrh projektu obranného vývoje MO ČR	počet stran: 34
příloha č. 3 – Takticko-technické požadavky	počet stran: 9
příloha č. 4 – Charakteristika projektu	počet stran: 5
příloha č. 5 – Katalogizační doložka	počet stran: 1

Poskytovatel: Příjemce: Ing. Jakub Papírník Digitálně podepsal Ing. Jakub Papírník Datum: 2022.04.27 12:09:14 +02'00'

JUDr. Pavlína ČERMÁKOVÁ
ředitelka
podepsáno elektronicky

Ing. Jakub PAPÍRNÍK
ředitel
podepsáno elektronicky

Všeobecné podmínky ke smlouvě o poskytnutí účelové podpory na řešení programového projektu

Článek 1
Řízení projektu

1. Příjemce vyvine veškeré nezbytné úsilí, aby dosáhl cílů uvedených v projektu a splnil veškeré závazky vůči poskytovateli.
2. Příjemce je povinen:
   a) použít poskytnuté prostředky výlučně na úhradu uznaných nákladů na činnosti ve výzkumu, vývoji a inovacích nebo v souvislosti s nimi a v souladu se Smlouvou a zákonem č. 130/2002 Sb.;
   b) neprodleně písemně informovat poskytovatele o skutečném zahájení řešení projektu;
   c) předávat poskytovateli doklady o projektu podle článku 5 těchto Všeobecných podmínek;
   d) neprodleně písemně informovat poskytovatele o každé okolnosti, která by mohla podstatně ovlivnit splnění cílů projektu, nejpozději však do 7 kalendářních dnů ode dne, kdy se o této okolnosti dozví;
   e) přijímat opatření pro řádné provádění svých závazků stanovených v Návrhu projektu;
   f) zúčastňovat se jednání, která byla svolána za účelem kontroly, sledování a hodnocení projektu prostřednictvím svých zástupců;
   g) předkládat poskytovateli všechny požadované údaje o řádném dodržování podmínek Smlouvy.
3. Návrh, včetně zdůvodnění, na změnu termínů jednotlivých etap řešení projektu je příjemce povinen předložit poskytovateli nejpozději do 30 kalendářních dnů před sjednanými termíny jejich ukončení. Poskytovatel je povinen do 20 pracovních dnů od doručení tento návrh schválit, odmítnout nebo vyzvat k jednání. Pokud tak poskytovatel ve stanovené lhůtě neučiní, má se za to, že s předloženým návrhem souhlasí.
4. I po splnění závazků ze Smlouvy, resp. v případě zániku Smlouvy, zůstávají v platnosti čl. 5 odst. 2 písm. A), čl. 7, 8, 12, 13 a čl. 14 odst. 5 a 6 Všeobecných podmínek.

Článek 2
Dodavatel a Další účastníci projektu

1. Není-li v návrhu projektu podrobně specifikována služba, pořízení hmotného nebo nehmotného majetku, a to včetně ceny a dodavatele, postupuje se při výběru tohoto dodavatele v souladu se zákonem č. 134/2016 Sb.
2. Smlouva o účasti na řešení projektu mezi příjemcem a dalšími účastníky projektu musí obsahovat právo poskytovatele na kontrolu dalších účastníků v takovém rozsahu, v jakém je má poskytovatel vůči příjemci.
3. Náklady všech dodavatelů poskytujících služby nesmějí překročit bez předchozího písemného souhlasu poskytovatele u projektu obranného výzkumu v souhrnu 20 % a u projektu obranného vývoje v souhrnu 30 % z poskytnuté podpory na projekt dle Smlouvy.

4. Členy řešitelského týmu a dodavateli poskytujícími služby nesmí být zaměstnanci a příslušníci organizační složky státu Ministerstvo obrany ČR, pokud činnost takových osob ve prospěch příjemce je předmětem jejich funkční náplně vyplývající z jejich pracovního nebo služebního zařazení v organizační složce státu Ministerstvo obrany ČR, ledaže na tyto osoby příjemce nežádá poskytnutí podpory.

Článek 3
Uznané náklady

1. Uznané náklady poskytovatel schválil jako náklady nutné k realizaci projektu, které budou vynaloženy během jeho řešení, budou zdůvodněné a prokazatelné.
2. Do uznaných nákladů se zahrnují položky podle § 2 odst. 2 písm. n) zákona č. 130/2002 Sb.
3. Poskytovatel může uznat kromě nákladů uvedených ve schváleném návrhu projektu i další neuvedené náklady, u kterých příjemce prokáže jejich nezbytnost pro řešení projektu.
4. Do uznaných nákladů nelze zahrnout především náklady podle čl. 2 odst. 4 těchto Všeobecných smluvních podmínek, dále zisk, daň z přidané hodnoty u těch příjemců, kteří jsou plátci daně z přidané hodnoty a uplatňující odpočet této daně nebo jeho poměrnou část, náklady na marketing (zejména reklama, dary, občerstvení), prodej a distribuci výrobků, úroky z dluhů, kurzovní ztráty, náklady na finanční pronájem (operativní leasing) a pronájem s následnou koupí (leasing), zahraniční služební cesty (např. veletrhy a konference, pokud tyto přímo nesouvisí s prezentací výsledku projektu) a další závazky nesouvisející s řešením projektu.
5. V průběhu řešení projektu může příjemce provést změnu pouze uvnitř jednotlivých položek vymezených ustanovením § 2 odst. 2 písm. m) zákona č. 130/2002 Sb. v rámci daného roku řešení projektu. O změně je příjemce povinen poskytovatele bezodkladně písemně informovat s přihlédnutím k odst. 7 tohoto článku.
6. O změnu mezi jednotlivými položkami vymezenými ustanovením § 2 odst. 2 písm. m) zákona č. 130/2002 Sb. je příjemce povinen v dostatečném časovém předstihu s přihlédnutím k odst. 7 tohoto článku předložit poskytovateli zdůvodněnou písemnou žádost. Poskytovatel je povinen do 30 kalendářních dnů od doručení tuto žádost schválit, odmítnout nebo vyzvat druhou smluvní stranu k jednání. Pokud tak poskytovatel ve stanovené lhůtě neučiní, má se za to, že s předloženým návrhem vyslovil souhlas.
7. Informaci o změně uznaných nákladů ve smyslu odst. 5 tohoto čl. a žádost o přerozdělení účelové podpory ve smyslu odst. 6 tohoto čl. příjemce doručí poskytovateli nejpozději do 15. října daného kalendářního roku, jinak změna nebude akceptována a žádost se považuje za zamítnutou.
8. Nastanou-li podstatné změny okolností týkající se řešení projektu, které příjemce nemohl předvídat a ani je nezpůsobil, požádá příjemce poskytovatele o změnu výše uznaných nákladů, nejpozději do 7 kalendářních dnů ode dne, kdy se o takových změnách dozvěděl. Žádost o změnu výše uznaných nákladů, bude řešena v souladu s ustanovením § 9 odst. 7 zákona č. 130/2002 Sb.

Článek 4
Čerpání podpory

1. V roce zahájení realizace projektu bude podpora poskytovatelem poskytnuta příjemci do 60 kalendářních dnů ode dne nabytí účinnosti Smlouvy formou dotace z výdajů na výzkum a vývoj přímým převodem z účtu poskytovatele na bankovní účet příjemce.

2. V následujících letech řešení projektu bude podpora poskytovatelem poskytnuta příjemci vždy do 60 kalendářních dnů od začátku příslušného kalendářního roku za podmínky, že příjemce řádně splnil závazky stanovené Smlouvou, zejména předložil průběžné zprávy o postupu řešení projektu, příslušné doklady o vynaložených nákladech nebo jiné podklady o projektu a tyto byly schváleny a za podmínky, že budou do informačního systému výzkumu, vývoje a inovací zařazeny údaje o projektu v souladu se zákonem o podpoře výzkumu a vývoje. V případě nesplnění závazků platí 60denní lhůta od jejich řádného splnění.
3. V případě, že příjemce nevyčerpá podporu pro daný kalendářní rok řešení, je povinen nevyčerpanou část vrátit na depozitní účet poskytovatele nejpozději do 14. února následujícího kalendářního roku.
4. V případech použití podpory poskytovatele nebo její části na jiný účel než je stanoveno ve Smlouvě je příjemce povinen ji v tomto rozsahu vrátit na depozitní účet poskytovatele nejpozději do 14. února následujícího kalendářního roku.
5. Platby a převody se považují za provedené dnem, kdy budou připsány na účet příjemce platby.

Článek 5
Ověření cílů a výsledků projektu, předkládání zpráv a dokladů

1. Ověření dosažení cílů a výsledků bude u projektů obranného výzkumu prováděno oponentním řízením k průběžným zprávám a závěrečné zprávě a kontrolními dny a u projektů experimentálního vývoje oponentním řízením k předběžnému a konečnému projektu, podnikovými, kontrolními a vojskovými zkouškami a kontrolními dny.
2. Zprávy a doklady o nákladech předkládá příjemce pouze poskytovateli.

A. Zprávy

Příjemce předkládá poskytovateli ke schválení následující zprávy (v písemné i elektronické podobě):

a) průběžné zprávy o postupu řešení projektu, tj. zprávy o postupu prací, vynaložených prostředcích, případných odchylkách od plánu práce a o dosažených výsledcích za uplynulé období. Přičemž první období vždy začíná zahájením projektu v daném roce a končí 31. prosince tohoto roku. Další období odpovídají kalendářním rokům řešení projektu;

b) neperiodické zprávy o splnění dílčích etap řešení projektu nebo o výsledcích řešení projektu, u nichž byly zahájeny kroky k zajištění jejich právní ochrany;

c) další zprávy s informacemi vyžadovanými poskytovatelem. Termín předání bude stanoven v příslušné žádosti;

d) závěrečnou zprávu o všech pracích, cílech, výsledcích a závěrech se shrnutím všech těchto uvedených bodů; závěrečná zpráva vhodná pro publikování musí být zpracována tak, aby poskytla třetím stranám dostatečnou informaci o výsledcích řešení projektu.

Zprávy uvedené v písm. b) a c) tohoto článku nesmějí být zveřejněny v plném znění. O rozsahu jejich zveřejnění rozhoduje poskytovatel. Obsah zpráv a lhůty pro jejich odevzdání musí splňovat pokyny poskytovatele.

Poskytovatel umožní příjemci přístup ke vzoru průběžné zprávy a závěrečné zprávy v elektronické podobě. Vzory průběžné zprávy a závěrečné zprávy jsou k dispozici na internetové adrese [redacted]

B. Prokázání nákladů

1. Příjemce prokazuje vynaložené náklady poskytovateli ve formě výkazu čerpání poskytnuté podpory za příslušný kalendářní rok. Poskytovatel umožní příjemci přístup ke vzoru výkazu čerpání poskytnuté podpory v elektronické podobě. Vzor výkazu čerpání poskytnuté podpory je k dispozici na internetové adrese [redacted]
2. Jako přílohu průběžné zprávy dále předkládá příjemce výkaz pořízených materiálových vstupů pro stavbu prototypu. Vzor výkazu pořízených materiálových vstupů pro stavbu prototypu je k dispozici na internetové adrese [redacted]
3. Příjemce je povinen vést pro příslušný projekt oddělenou evidenci o uznaných nákladech podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a v rámci této evidence sledovat náklady hrazené z poskytnuté podpory.

C. Společná ustanovení

1. Každá průběžná zpráva musí být předložena poskytovateli v termínu stanoveném v pokynech k provedení oponentních řízení, které budou k dispozici na internetové adrese [redacted] Současně příjemce předloží jako samostatný dokument výkaz čerpání poskytnuté podpory v členění podle § 2 odst. 2 písm. m) zákona č. 130/2002 Sb..
2. Neperiodické zprávy o splnění dílčích etap řešení projektu nebo o výsledcích řešení projektu předkládá příjemce poskytovateli do 15 kalendářních dnů od ukončení etapy.
3. Termín předání dalších zpráv s informacemi vyžadovanými poskytovatelem bude stanoven v příslušné žádosti.
4. Závěrečná zpráva musí být předložena nejpozději do 30 kalendářních dnů od ukončení řešení projektu.
5. Současně příjemce předloží jako samostatný dokument výkaz čerpání poskytnuté podpory za celou dobu řešení projektu (od zahájení do předčasného zastavení nebo ukončení) v členění podle § 2 odst. 2 písm. m) zákona č. 130/2002 Sb.
6. Na základě pověření poskytovatele je příjemce povinen zorganizovat oponentní řízení k dosaženým výsledkům, průběžné a závěrečné zprávě a dalším předloženým materiálům s tím, že výběr osob oponentů včetně jejich odměnění je plně v kompetenci poskytovatele a konečný termín oponentního řízení určuje poskytovatel. Pokyny k provedení oponentních řízení budou k dispozici na internetové adrese [redacted]
7. Bude-li řešení projektu zastaveno před termínem uvedeným ve Smlouvě, platí ustanovení o závěrečné zprávě a příslušných dokladech o nákladech pro období do termínu předčasného ukončení projektu.

Článek 6
Odborní poradci

1. Poskytovatel si může za účelem kontroly, sledování a hodnocení projektu přizvat nezávislé odborné poradce.
2. Poskytovatel odborné poradce písemně zaváže k zachovávání mlčenlivosti o informacích, které jim budou poskytnuty a k závazku nevyužívat tyto informace ve prospěch svůj nebo třetích osob.
3. Poskytovatel seznámí příjemce se jmenováním odborných poradců a umožní příjemci vznést námitky vůči osobám odborných poradců ve stanovené lhůtě. Poskytovatel tyto námitky posoudí a shledá-li je oprávněnými, odvolá jmenovaného odborného poradce a jmenuje jiného.

Článek 7
Vlastnictví hmotného majetku pořízeného pro výzkum a vývoj, práva k výsledkům a jejich využití

1. Vlastníkem materiálu nebo prostředků nutných k vyřešení daného projektu pořízeného z podpory je příjemce v rozsahu Smlouvy a zákona č. 130/2002 Sb.
2. Nelze-li výsledky projektu chránit podle zvláštních právních předpisů, je vlastníkem výsledků poskytovatel a jejich zveřejnění a využití je možné pouze s předchozím písemným souhlasem poskytovatele.
3. Lze-li výsledky projektu chránit podle zvláštních právních předpisů, potom je příjemce povinen bezodkladně uplatnit vlastnické právo k těmto výsledkům, zajistit jejich právní ochranu a po jejím udělení vlastnické právo převést na poskytovatele. Příjemce má nárok na úhradu prokazatelných nákladů s tím spojených, pokud nebyly součástí uznaných nákladů.
4. Vznikne-li jako výsledek projektu či jako nedílná součást výsledků projektu autorské dílo, popř. zaměstnanecké dílo podle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména počítačový program nebo software, je příjemce povinen s poskytovatelem ve lhůtě pro řešení projektu uzavřít bezúplatnou licenční smlouvu podle § 2358 a násl. zákona č. 89/2012 Sb., kterou poskytne poskytovateli výhradní právo v územně, časově a množstevně neomezeném rozsahu užívat, upravovat či jinak měnit toto autorské dílo.
5. Práva k výsledkům a jejich využití se řídí dle § 16 zákona č. 130/2002 Sb.

Článek 8
Odpovědnost za škody a okolnosti vylučující odpovědnost

1. Příjemce odpovídá poskytovateli za škodu, kterou mu způsobí v souvislosti s plněním předmětu této Smlouvy.
2. Smluvní strany se dohodly, že v případě náhrady škody se bude hradit pouze skutečná prokazatelně vzniklá škoda.
3. Nastanou-li skutečnosti, které vylučují odpovědnost jedné ze smluvních stran a které způsobí či mohou způsobit podstatné zpoždění termínů nebo jiného termínu podle této smlouvy, či zánik nebo zrušení závazků podle této smlouvy (vyšší moc), jsou smluvní strany povinny se neprodleně o těchto skutečnostech vylučujících odpovědnost informovat a vstoupit do jednání ohledně řešení vzniklé situace. Smluvní strany nejsou oprávněny takto vzniklé situace jakkoliv zneužít ve svůj prospěch a jsou povinny v dobré víře usilovat o dosažení přijatelného řešení, a to v co nejkratší možné době. V případě porušení této povinnosti kteroukoliv ze smluvních stran se má za to, že dotčená smluvní strana je v prodlení s plněním svých povinností dle této smlouvy.
4. Za okolnosti vylučující odpovědnost smluvních stran za prodlení s plněním smluvních závazků dle této smlouvy jsou považovány takové překážky, které nastanou nezávisle na vůli povinné smluvní strany a brání jí ve splnění její povinnosti z této smlouvy, jestliže nelze rozumně předpokládat, že by povinná smluvní strana takovou překážku nebo její následky odvrátila nebo překonala a dále že by v době vzniku smluvních závazků z této smlouvy vznik či existenci těchto překážek předpokládala.
5. V případě, že nedojde k dohodě smluvních stran, termíny plnění jednotlivých povinností podle této smlouvy dotčené okolností vylučující odpovědnost se prodlužují o dobu, po kterou okolnost vylučující odpovědnost trvala.

6. Odpovědnost nevylučuje překážka, která vznikla teprve v době, kdy povinná smluvní strana byla již v prodlení s plněním své povinnosti, či vznikla z jejích hospodářských poměrů.

7. Účinky vylučující odpovědnost jsou omezeny pouze na dobu, dokud trvá příslušná překážka, s níž jsou tyto účinky spojeny. Dobu trvání příslušné překážky je dotčena smluvní strana povinna objektivně prokázat.

Článek 9
Uplatnění katalogizační doložky

1. Příjemce bere na vědomí, že výsledky projektu definované ve Smlouvě a dále položky, které budou poskytovatelem označeny ve schváleném konečném projektu jako položka zásobování (příloha konečného projektu), budou předmětem katalogizace dle § 9 a násl. zákona č. 309/2000 Sb., o obranné standardizaci, katalogizaci a státním ověřování jakosti výrobků a služeb určených k zajištění obrany státu a o změně živnostenského zákona, ve znění pozdějších předpisů (dále je „zákon č. 309/2000 Sb.“).

2. Příjemce se zavazuje, že umožní řádně provést katalogizaci, tj. dodá Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti (dále jen „Úř OSK SOJ“) návrh katalogizačních dat zpracovaných agenturou podle § 13 a § 14 zákona č. 309/2000 Sb., na výsledky projektu, které jsou výsledkem řešení projektu podle Smlouvy. Předání návrhu katalogizačních dat je součástí plnění povinností příjemce dle této Smlouvy a příjemce nemá nárok na úhradu nákladů spojených s vypracováním katalogizačních dat. Zásady pro jejich zpracování jsou uvedeny v Katalogizační doložce.

3. Příjemce se zavazuje zpřístupnit či zabezpečit zpřístupnění dokumentace ke zpracování katalogizačních dat agentuře a k případnému ověření nebo doplnění katalogizačních dat Úř OSK SOJ.

Článek 10
Poskytování informací

1. Podpora je poskytována za podmínky zveřejňování pravdivých a včasných informací příjemcem o prováděném řešení projektu a jeho výsledcích prostřednictvím informačního systému výzkumu, vývoje a inovací dle § 12 zákona č. 130/2002 Sb.

2. Příjemce plní povinnost poskytování informací podle odst. 1 tohoto článku prostřednictvím poskytovatele, kterému předává údaje o projektu nebo údaje o získaných poznatcích ke zveřejnění do informačního systému výzkumu, vývoje a inovací.

3. Při změně Smlouvy je příjemce povinen předat poskytovateli informace o změně údajů zveřejňovaných v informačním systému výzkumu, vývoje a inovací.

4. Údaje je příjemce povinen doručit poskytovateli v písemné a elektronické podobě, a to nejpozději do 15 kalendářních dnů ode dne, kdy změna nastala nebo byla poskytovateli oznámena.

5. Pokud je předmět řešení projektu předmětem obchodního tajemství nebo utajovanou informací podle zvláštního právního předpisu, musí poskytovatel a příjemce poskytnout ke zveřejnění konkrétní informace o projektu a poznatcích ve zveřejnitelné podobě. Pokud je předmět řešení projektu utajovanou informací, předá poskytovatel i příjemce úplné údaje o projektu a poznatcích postupem stanoveným zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Článek 11
Zachování mlčenlivosti

1. Smluvní strany jsou povinny zajistit mlčenlivost o údajích, podkladech a vnesených právech vztahujících se k výsledkům projektu, které jim byly poskytnuty a jejichž předání dalším subjektům by mohlo být pro toho, kdo je poskytl, nevýhodné.
2. Závazek mlčenlivosti končí:
   a) pokud se obsah těchto údajů, podkladů a vnesených práv stane veřejně přístupným, a to na základě jiných závazků prováděných nad rámec Smlouvy nebo na základě opatření, která nesouvisejí s předmětem smlouvy;
   b) sdělením těchto údajů, podkladů a vnesených práv bez požadavku mlčenlivosti nebo pozdějším odvoláním požadavku mlčenlivosti těmi, kteří mají právo takto učinit.
3. Pokud jsou smluvní strany na základě Smlouvy oprávněny předávat údaje, podklady a vnesená práva dalším osobám, jsou povinny zajistit, aby tyto osoby zachovávaly mlčenlivost a veškeré údaje používaly jen k účelům, k nimž jim byly předány.

Článek 12
Kontroly

1. Příjemce je povinen uchovávat a na požádání zpřístupnit poskytovateli informace a dokumenty vztahující se k řešení projektu. Dokumenty vztahující se k řešení projektu je příjemce povinen uchovávat nejméně po dobu 10 let ode dne ukončení řešení projektu.
2. Poskytovatel je povinen provádět kontrolu plnění cílů projektu, včetně kontroly čerpání a využívání podpory, účelnosti vynaložených nákladů projektu podle uzavřené Smlouvy nebo rozhodnutí o poskytnutí podpory. Povinností příjemce je tuto kontrolu umožnit.
3. Kontrola podle odstavce 2 včetně zhodnocení dosažených výsledků a jejich právní ochrany se provádí vždy po ukončení řešení projektu. V případě, že doba, po kterou se poskytuje podpora, je delší než dva roky, je poskytovatel povinen provést kontrolu podle odstavce 2 rovněž nejméně 1x v průběhu řešení projektu.
4. Finanční kontrola je prováděna v souladu se zákonem č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, vyhláškou č. 416/2004 Sb., kterou se provádí zákon o finanční kontrole, a zákonem č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.
5. Osobám provádějícím kontrolu je příjemce povinen poskytnout pro účely kontroly volný přístup na pracoviště příjemce k osobám podílejícím se na řešení projektu, ke všem dokumentům, počítačovým záznamům a zařízením, které přísluší k projektu.

Článek 13
Sankční ujednání

1. Je-li řešení projektu zahájeno se zpožděním zaviněným příjemcem, v jehož důsledku nebude na řešení projektu vyčerpána část podpory určená pro příslušný kalendářní rok a nevyčerpané prostředky budou vráceny na účet stanovený poskytovatelem, je poskytovatel oprávněn požadovat úhradu smluvní pokuty ve výši 10 % z vrácené částky.
2. V případě, že příjemce provede změnu uznaných nákladů v rozporu s ustanovením čl. 3 těchto Všeobecných podmínek, je příjemce povinen uhradit poskytovateli smluvní pokutu v plné výši částky překračující jeho oprávnění.

3. Nedodrží-li příjemce termíny zaslání zpráv a výkazů čerpání poskytnuté podpory a plnění jednotlivých etap řešení projektu, je povinen uhradit poskytovateli za každý den prodlení smluvní pokutu ve výši 0,1 % z výše podpory poskytnuté pro příslušný kalendářní rok.
4. Nedodrží-li příjemce ustanovení čl. 7 odst. 2 těchto Všeobecných podmínek, je povinen uhradit poskytovateli smluvní pokutu ve výši 5 % z celkové výše uznaných nákladů.
5. V případech, kdy by byly po ukončení Smlouvy vůči příjemci při finanční kontrole zjištěny závažné finanční nesrovnalosti v souvislosti s užíváním poskytnuté podpory, může poskytovatel požadovat od příjemce vrácení celé poskytnuté podpory. Vrácená podpora bude zatížena smluvní pokutou ve výši 5 % z celkové poskytnuté podpory.
6. Právo na smluvní pokutu vzniká oprávněné straně od prvního dne následujícího po porušení smluvní povinnosti. Smluvní pokuta je splatná do 30 kalendářních dnů ode dne doručení jejího vyúčtování povinné smluvní straně.
7. Smluvní pokuty hradí povinná strana bez ohledu na to, zda a v jaké výši vznikla druhé straně v této souvislosti škoda, která je vymahatelná samostatně vedle smluvní pokuty v plné výši.

Článek 14
Ukončení Smlouvy

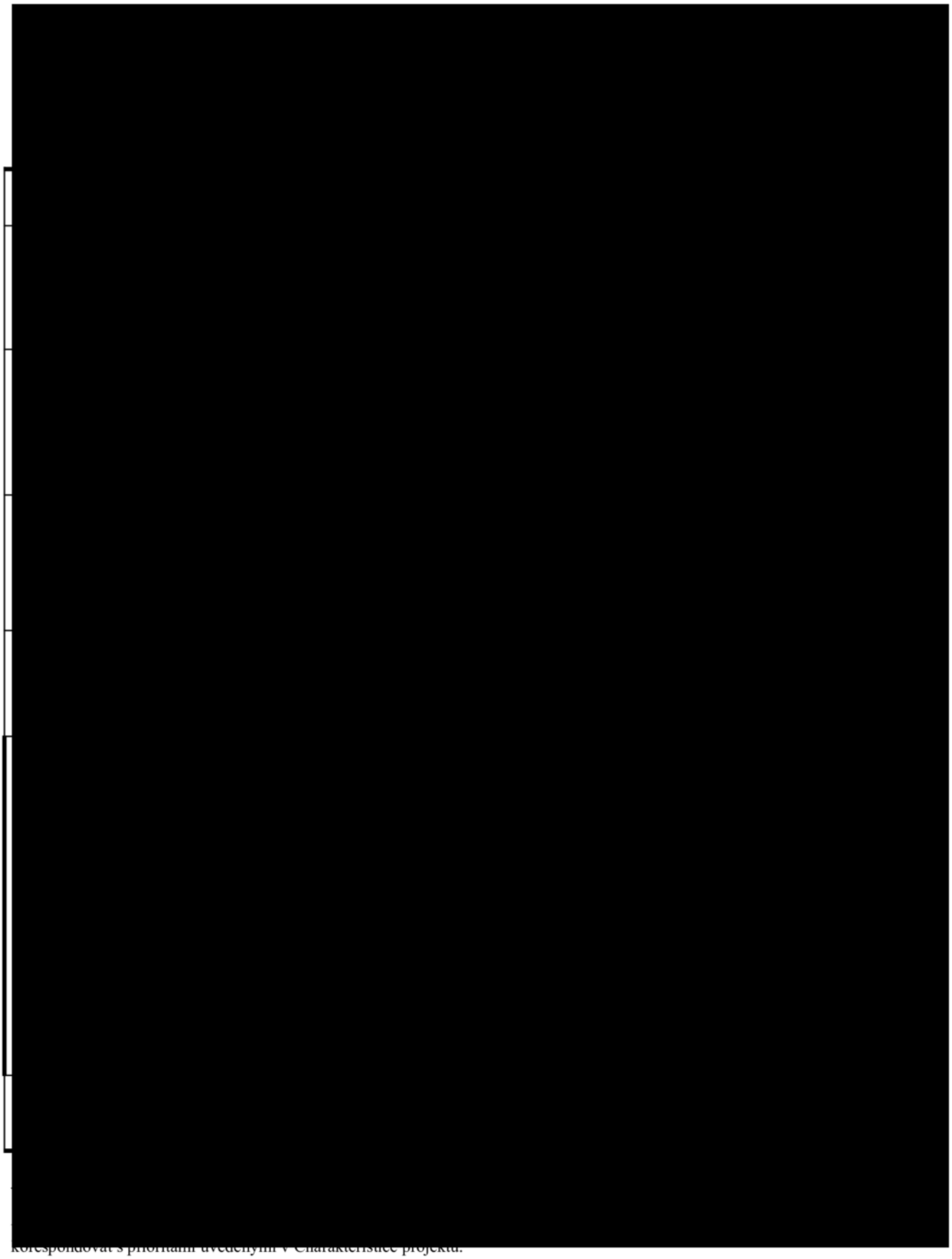
1. Příjemce a poskytovatel můžou písemně vypovědět Smlouvu ze závažných důvodů, které podstatně ovlivňují řešení projektu, nebo v případě, kdy se výrazně sníží možnost využití poznatků projektu. Výpovědní lhůta je dvouměsíční a počíná běžet první den měsíce následujícího po doručení výpovědi.
2. Poskytovatel může odstoupit od Smlouvy, jestliže:
   a) řešení projektu nebylo zahájeno do 60 kalendářních dnů ode dne nabytí účinnosti Smlouvy a nově navrhovaný termín zahájení řešení nebyl poskytovatelem akceptován;
   b) příjemce nedostál v plném rozsahu svým závazkům ani poté, co jej poskytovatel písemně vyzval, aby své závazky splnil nejpozději do 30 kalendářních dnů od doručení výzvy;
   c) oponentní rada nedoporučila pokračovat v řešení projektu a poskytovatel tento návrh schválil;
   d) zahájení insolvenčního řízení nebo řízení o likvidaci vedlo k přechodnému nebo definitivnímu ukončení činnosti příjemce;
   e) používá podporu v rozporu s jejím účelem.
3. Poskytovatel může odstoupit od Smlouvy v případě, kdy příjemce poskytl nepravdivé údaje nebo se dopustil záměrného opomenutí s cílem získat finanční podporu poskytovatele nebo jinou výhodu ze Smlouvy.
4. Příjemce po obdržení oznámení o odstoupení poskytovatele od Smlouvy provede všechna nezbytná opatření k tomu, aby své závazky při řešení projektu zcela vypořádal.
5. Při odstoupení od Smlouvy:
   a) podle odst. 2 tohoto článku mohou být uznány jen náklady za poskytovatelem schválené činnosti konané v souvislosti s řešením projektu, které byly konány před vznikem důvodu pro odstoupení od Smlouvy. Dále mohou být uznány i náklady, které byly uznány za způsobilé před termínem odstoupení;

b) podle odst. 3 tohoto článku je příjemce povinen vrátit poskytnutou podporu v plné výši; prostředky požadované k vrácení budou zatíženy smluvní pokutou ve výši 5 % z celkové výše poskytnuté podpory.

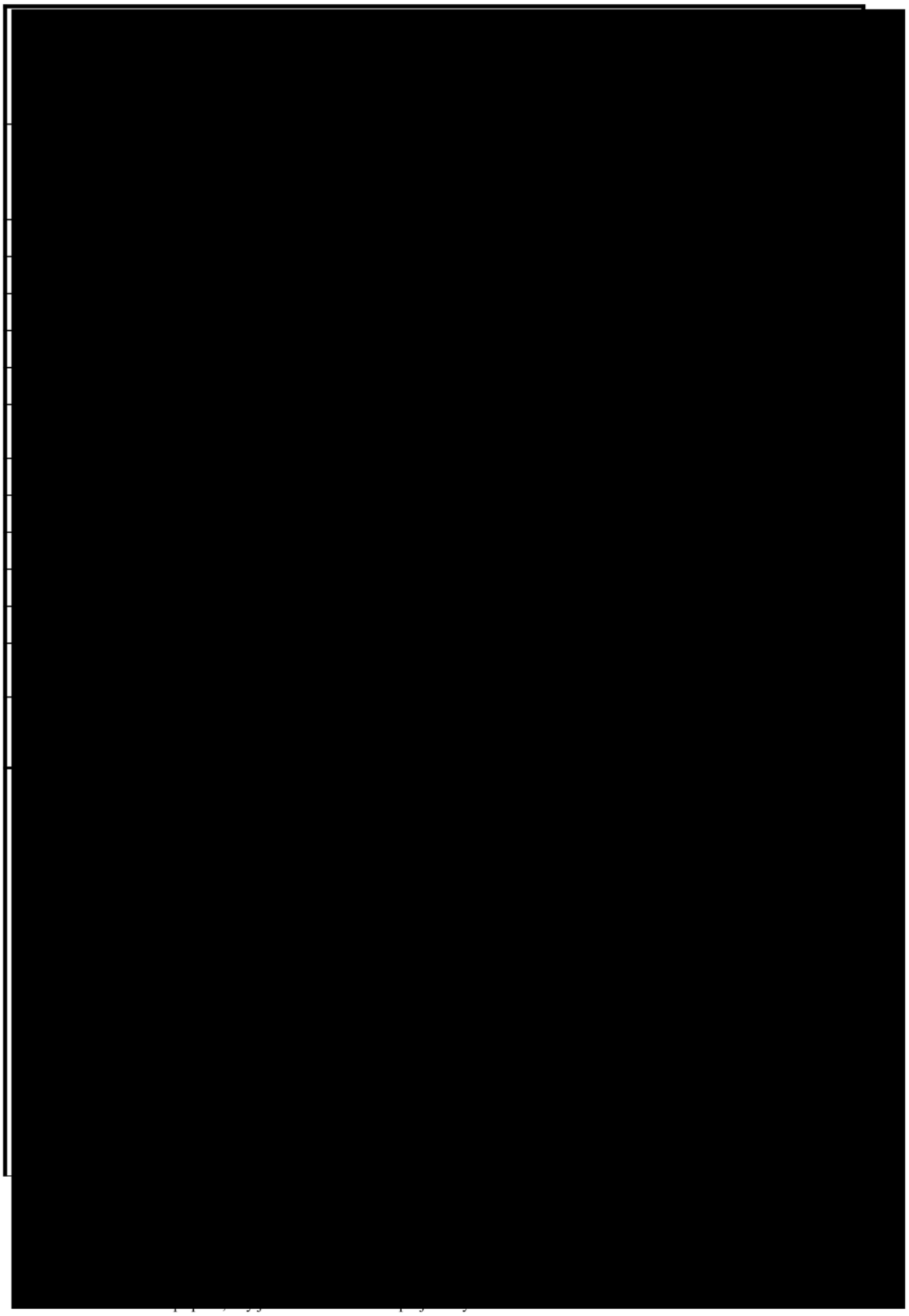
6. Při vypovězení Smlouvy podle odst. 1 tohoto článku je příjemce povinen vrátit poskytovateli poskytnutou podporu sníženou o uznané náklady za poskytovatelem schválené výstupy z projektu, které byly vynaloženy příjemcem před termínem doručení výpovědi poskytovatele, nebo vzniku důvodů pro výpověď na straně příjemce. Dále může být vrácená podpora snížena o poskytovatelem uznané náklady, které byly vynaloženy v dobré víře a uznány poskytovatelem za platné po termínu doručení výpovědi příjemci.

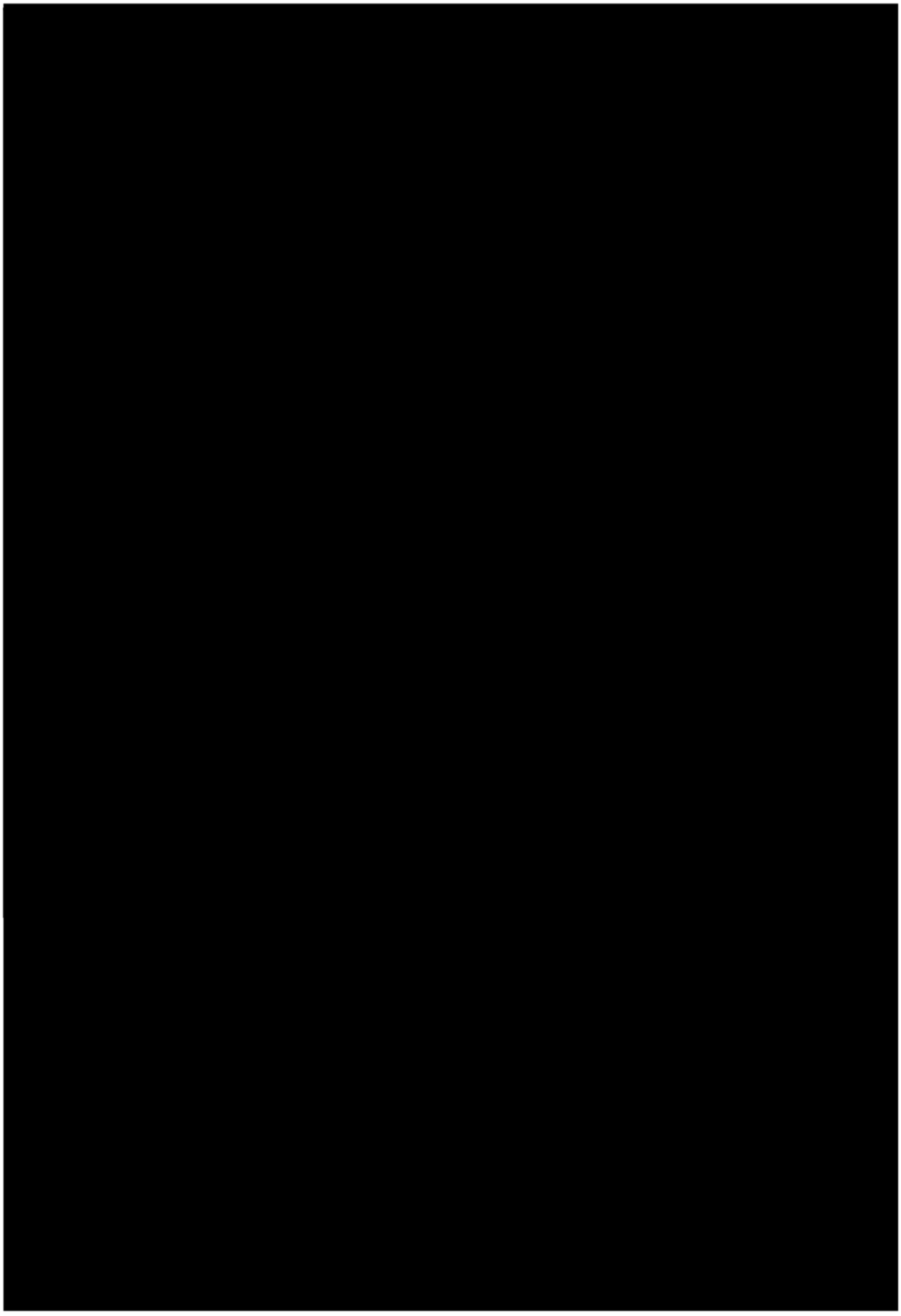
Příloha č. 2 ke smlouvě č. 2201 5 7370
Počet stran: 34

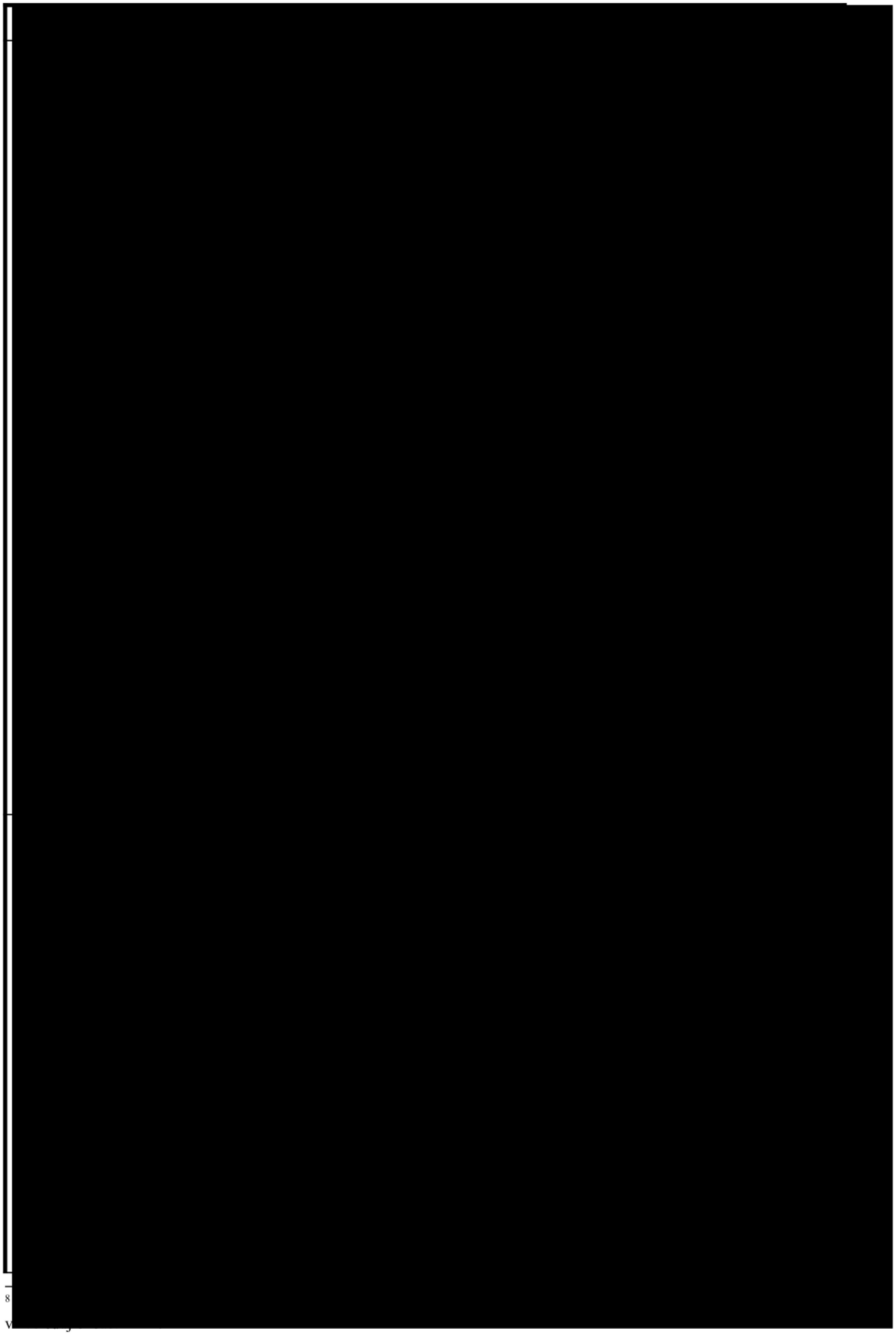
[redacted]

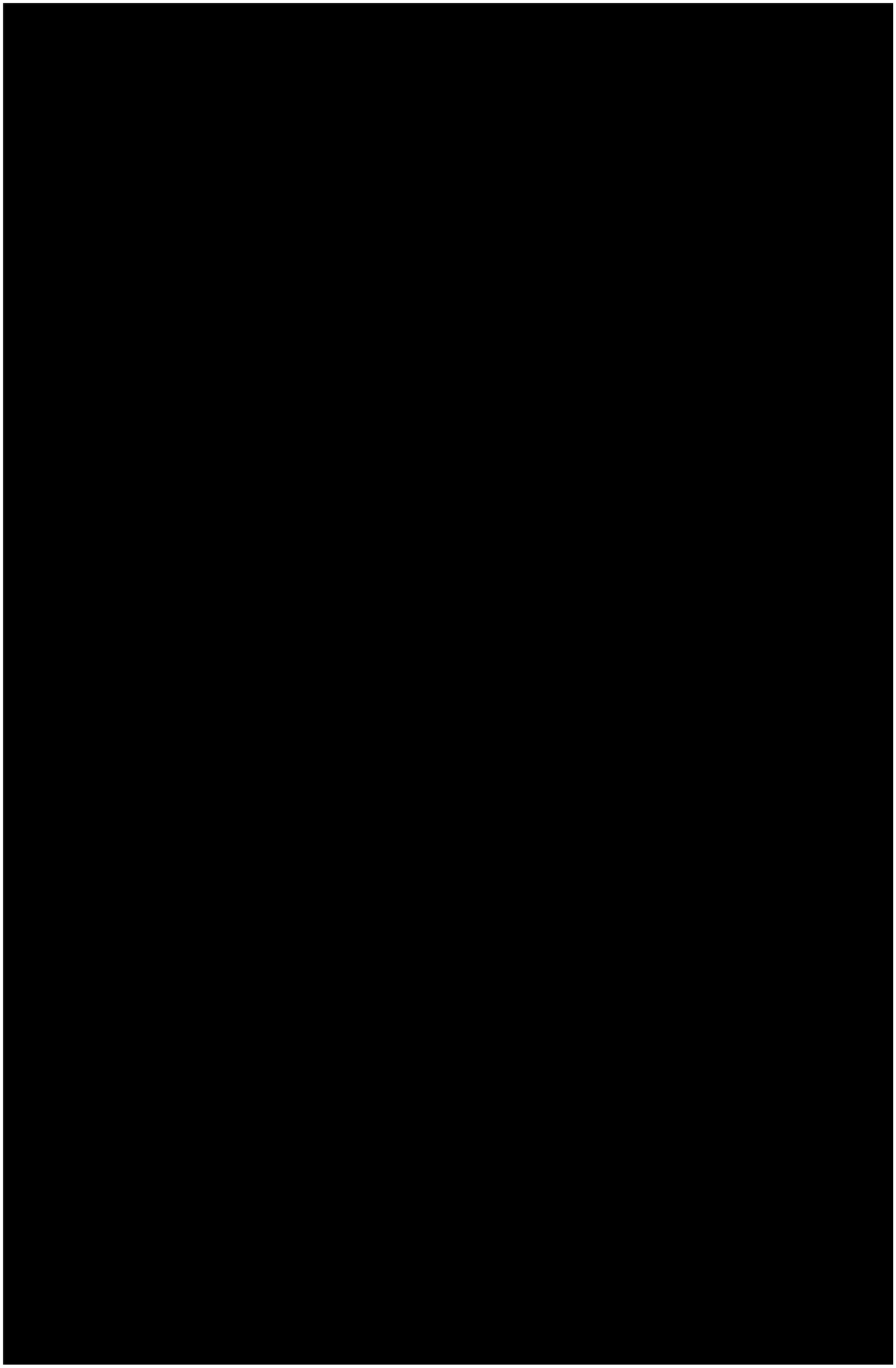


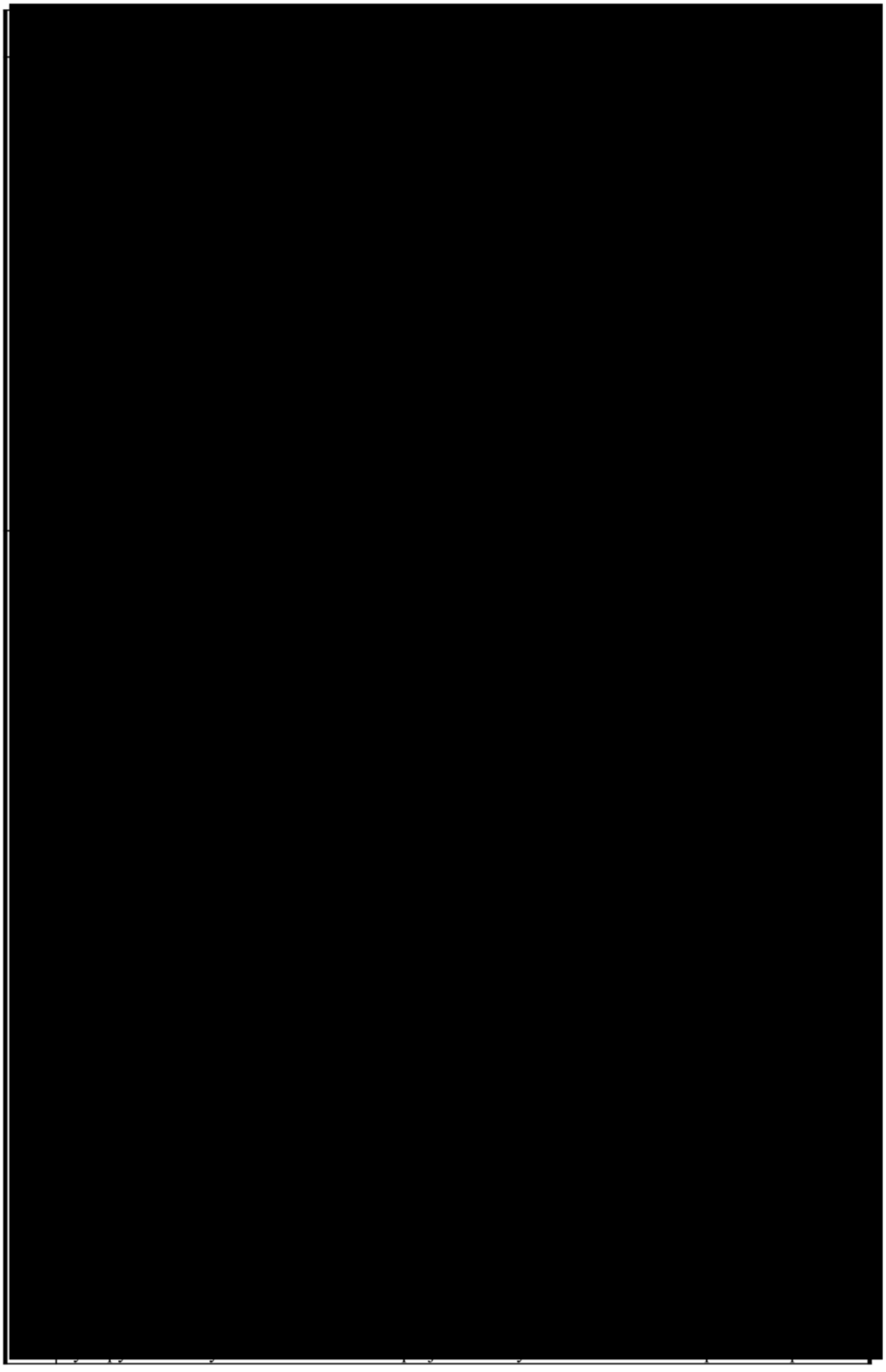
korespondovat s prioritami uvedenými v Charakteristice projektu.

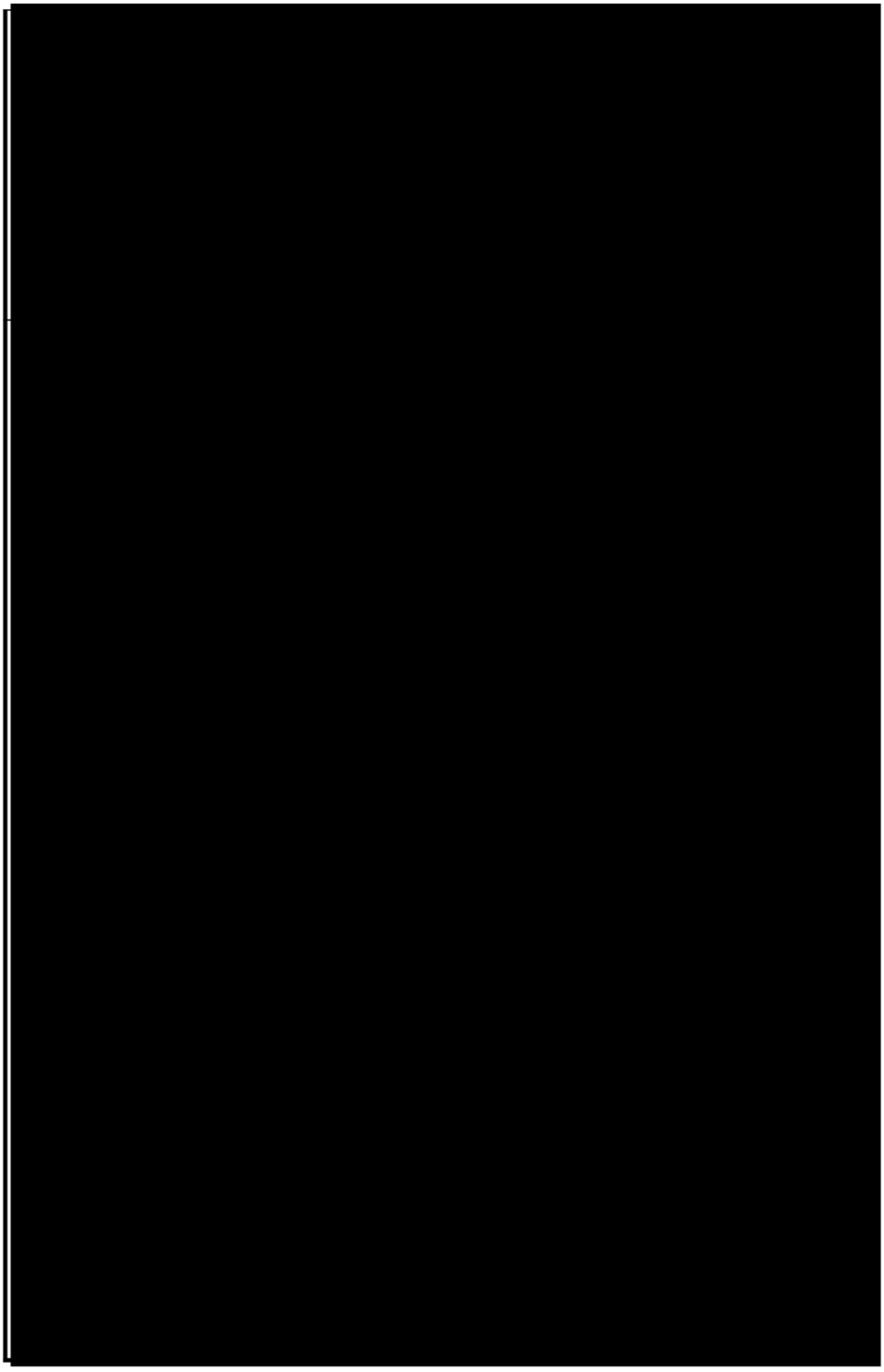


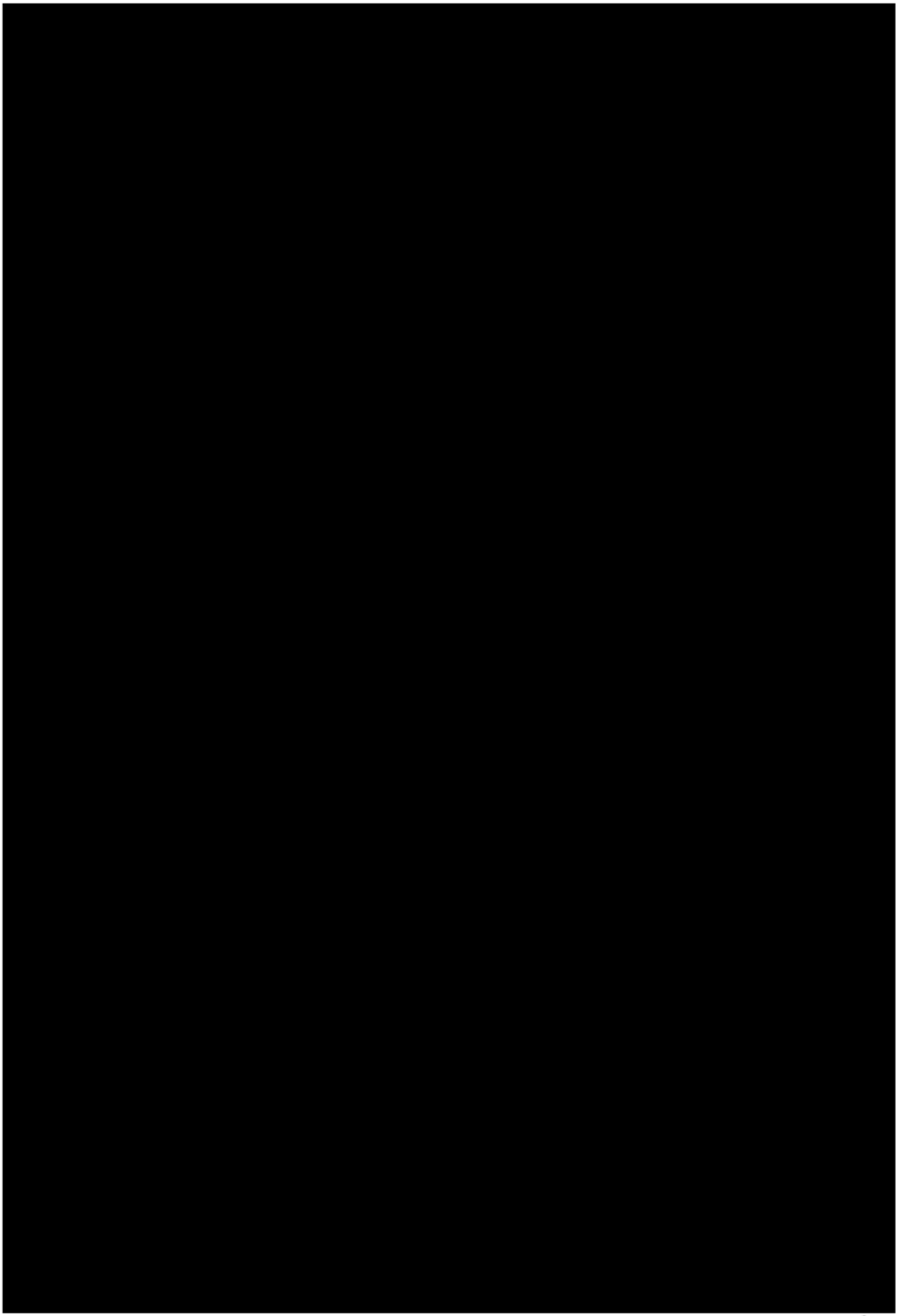


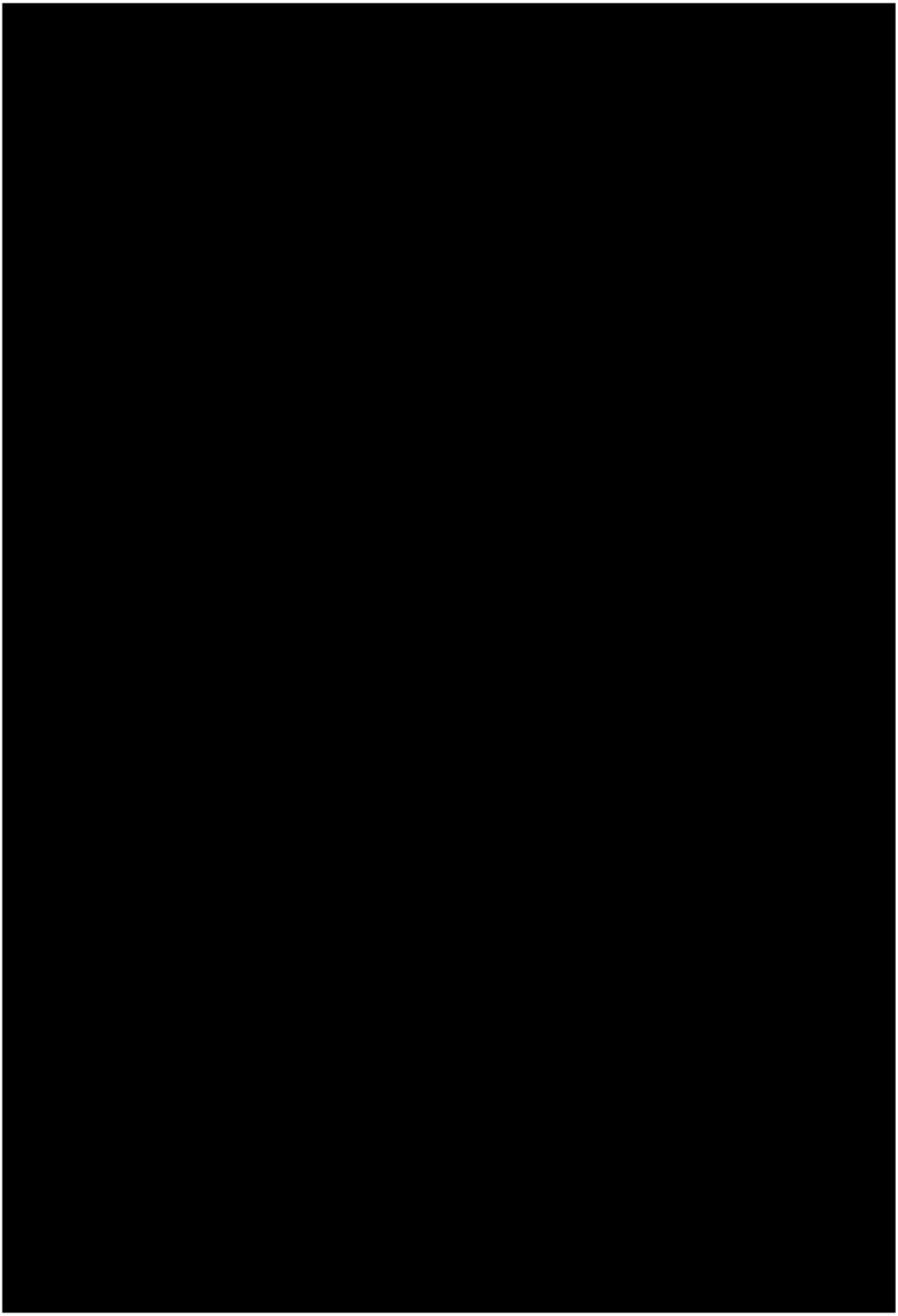


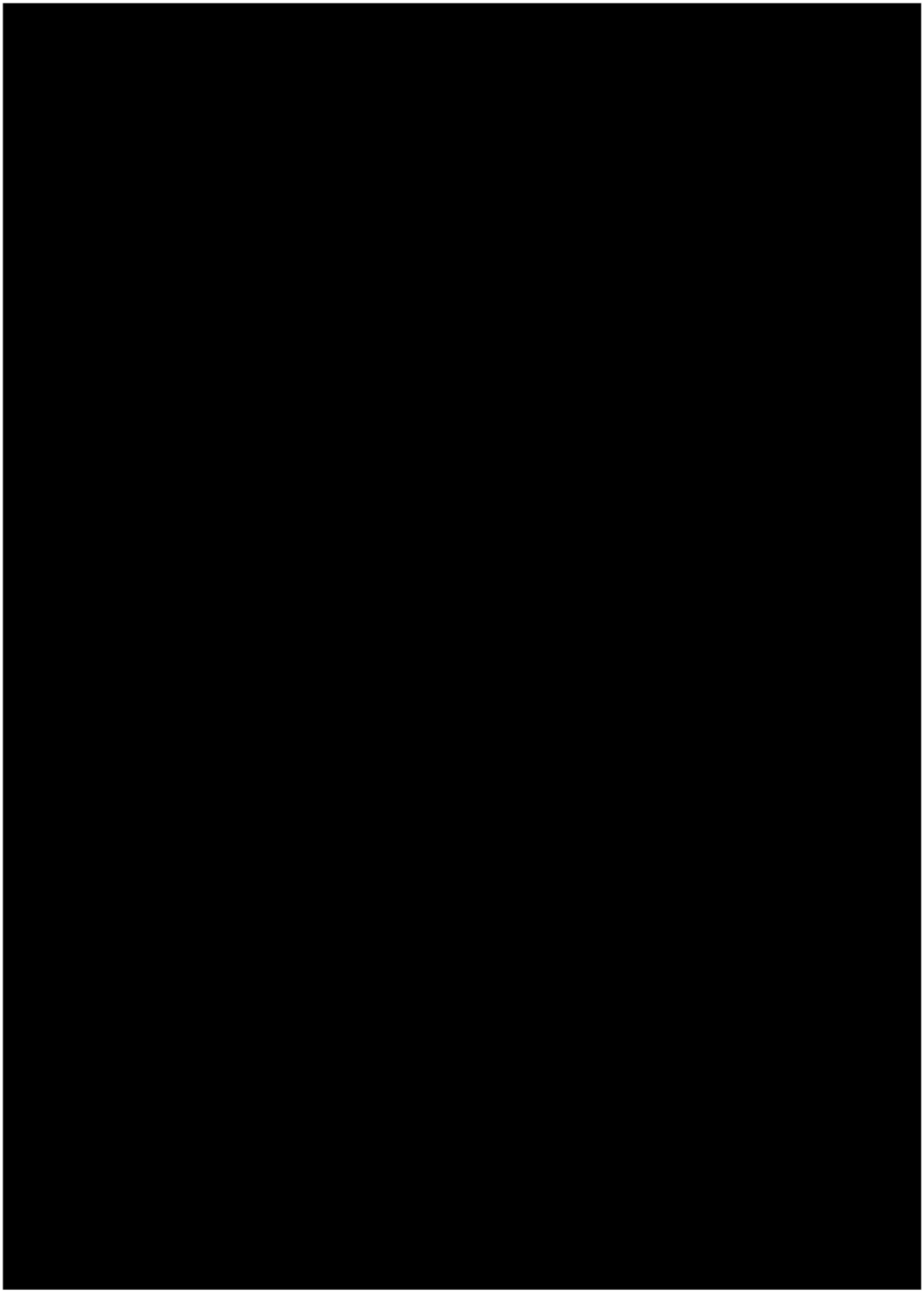


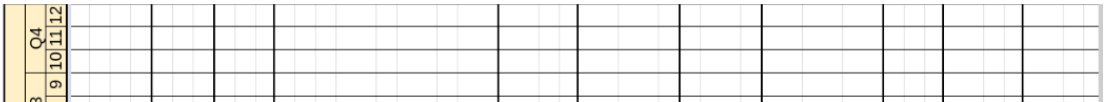


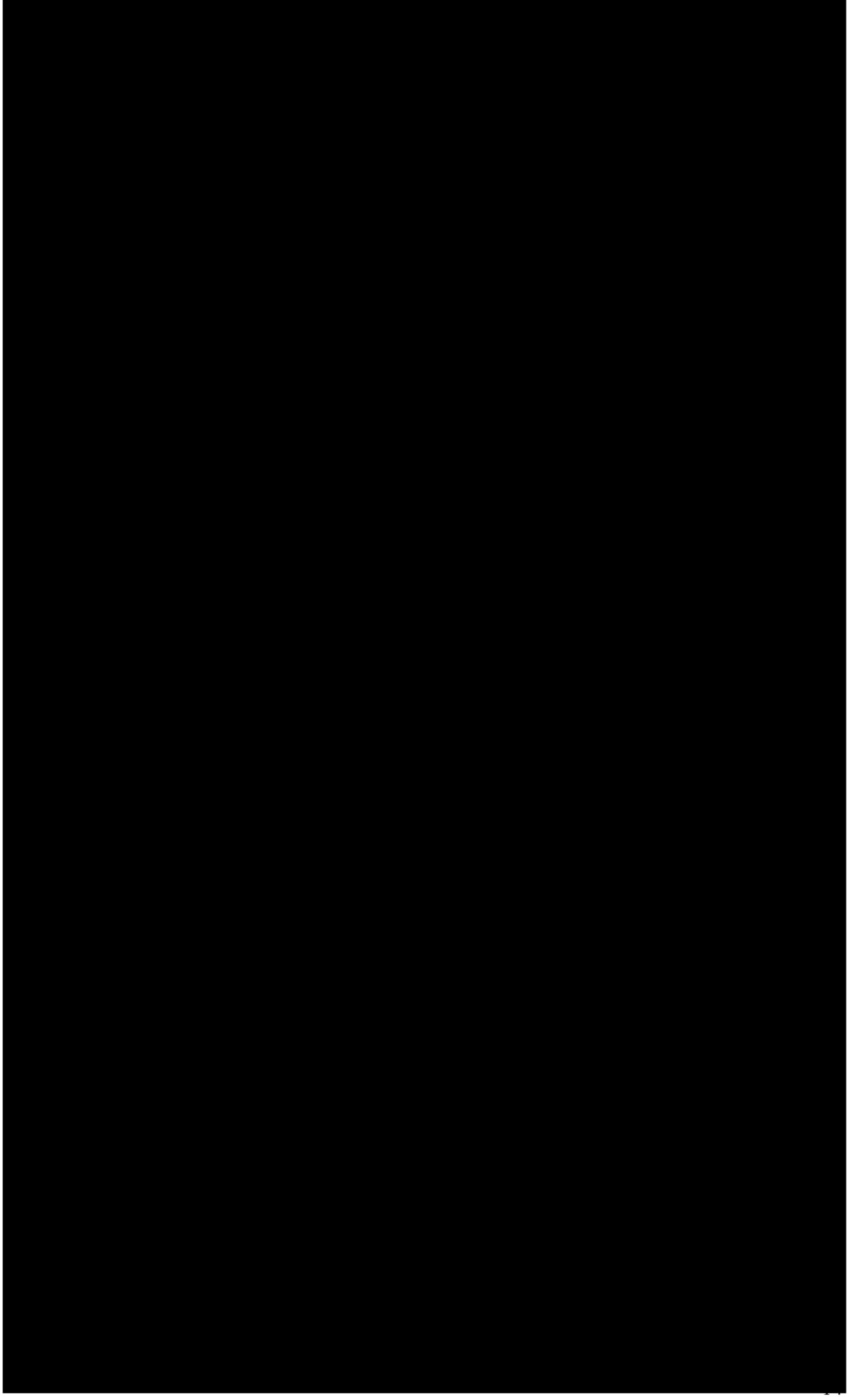


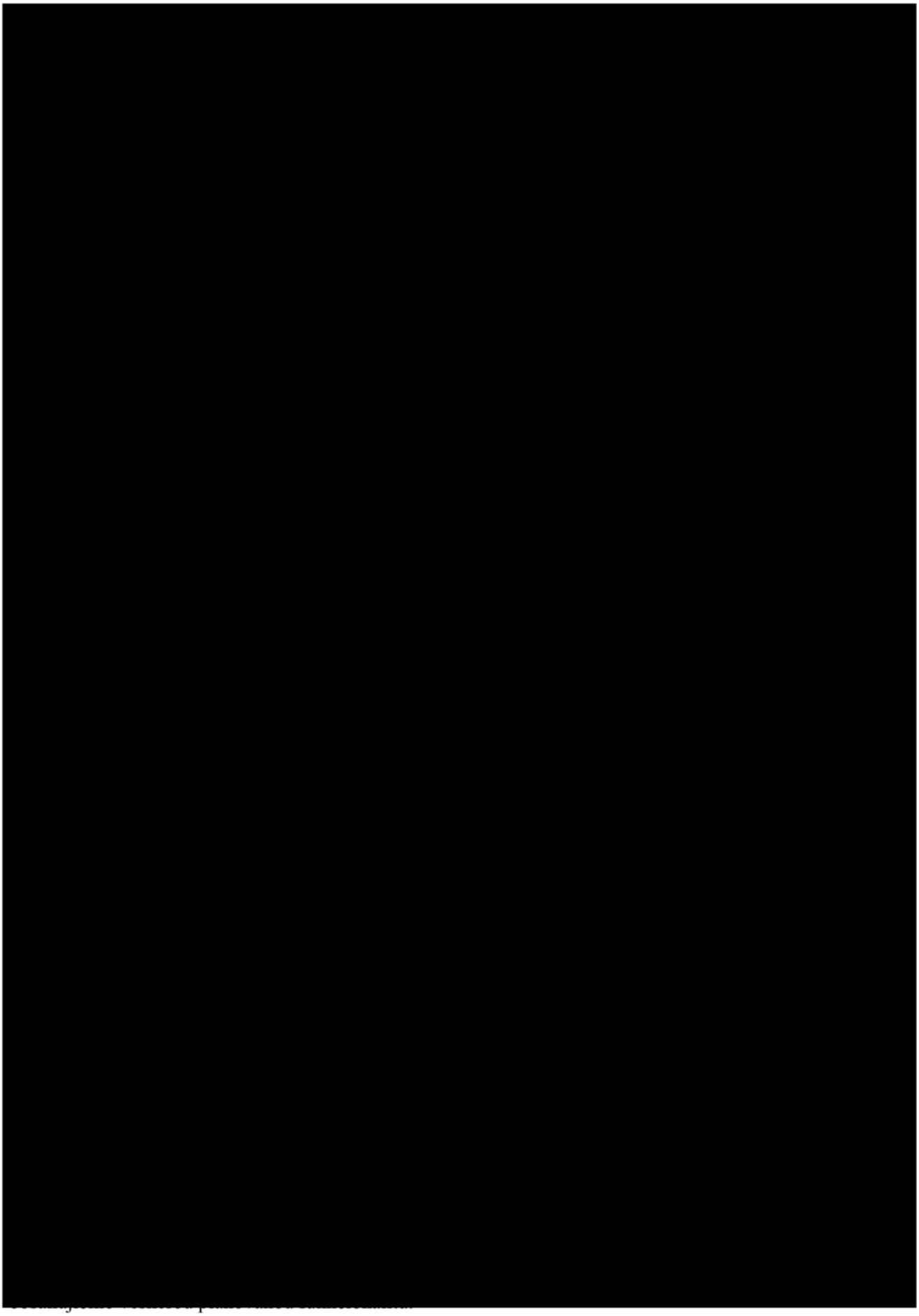


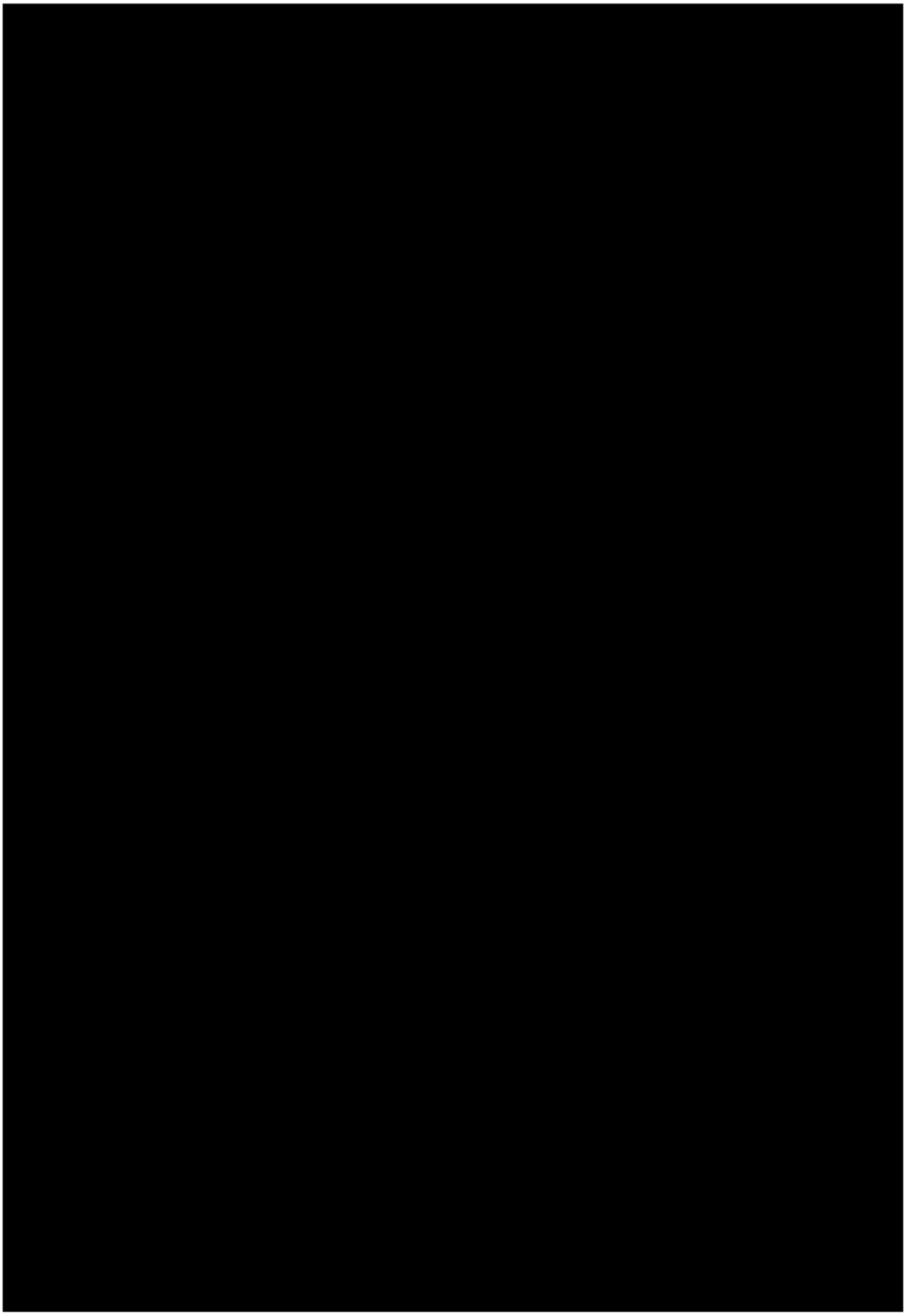


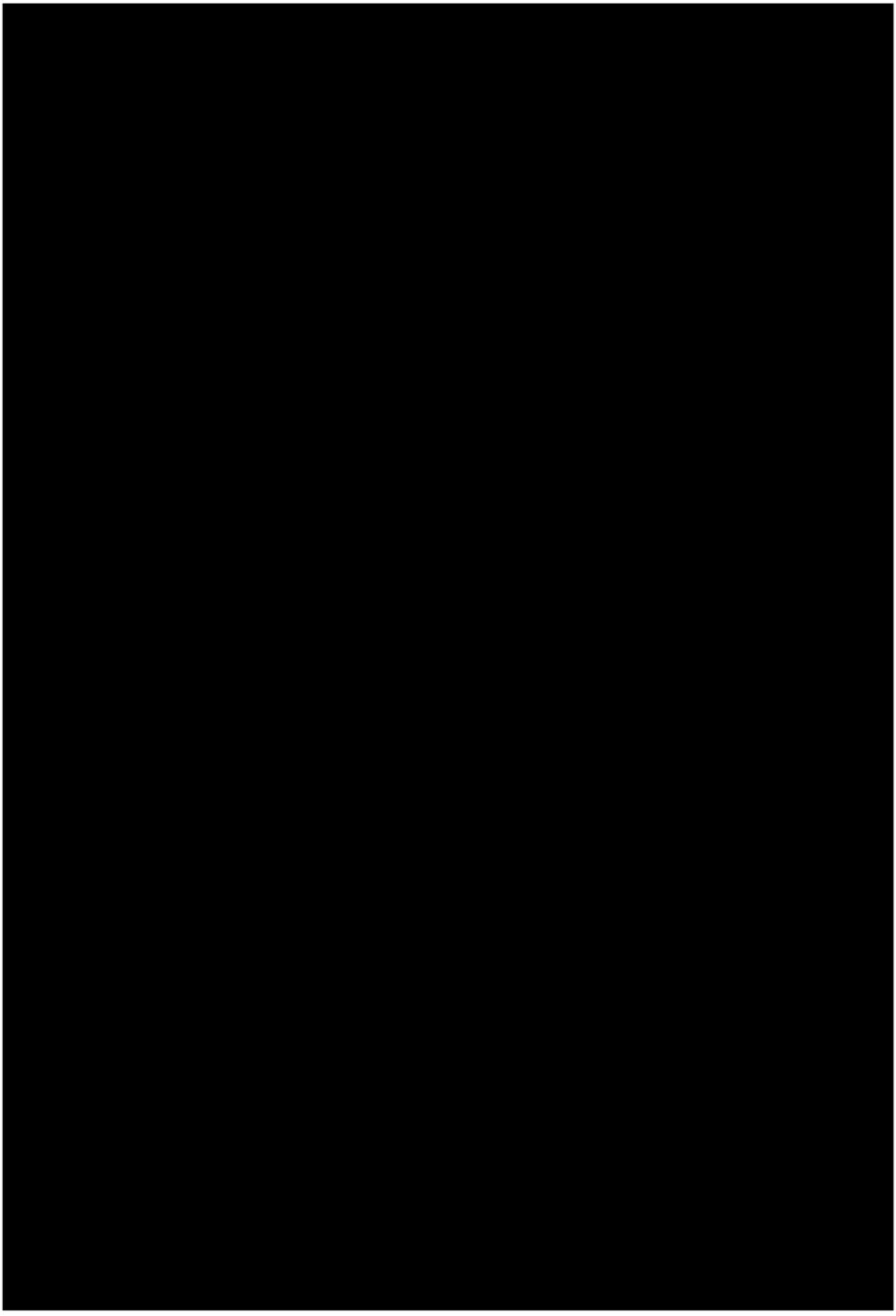


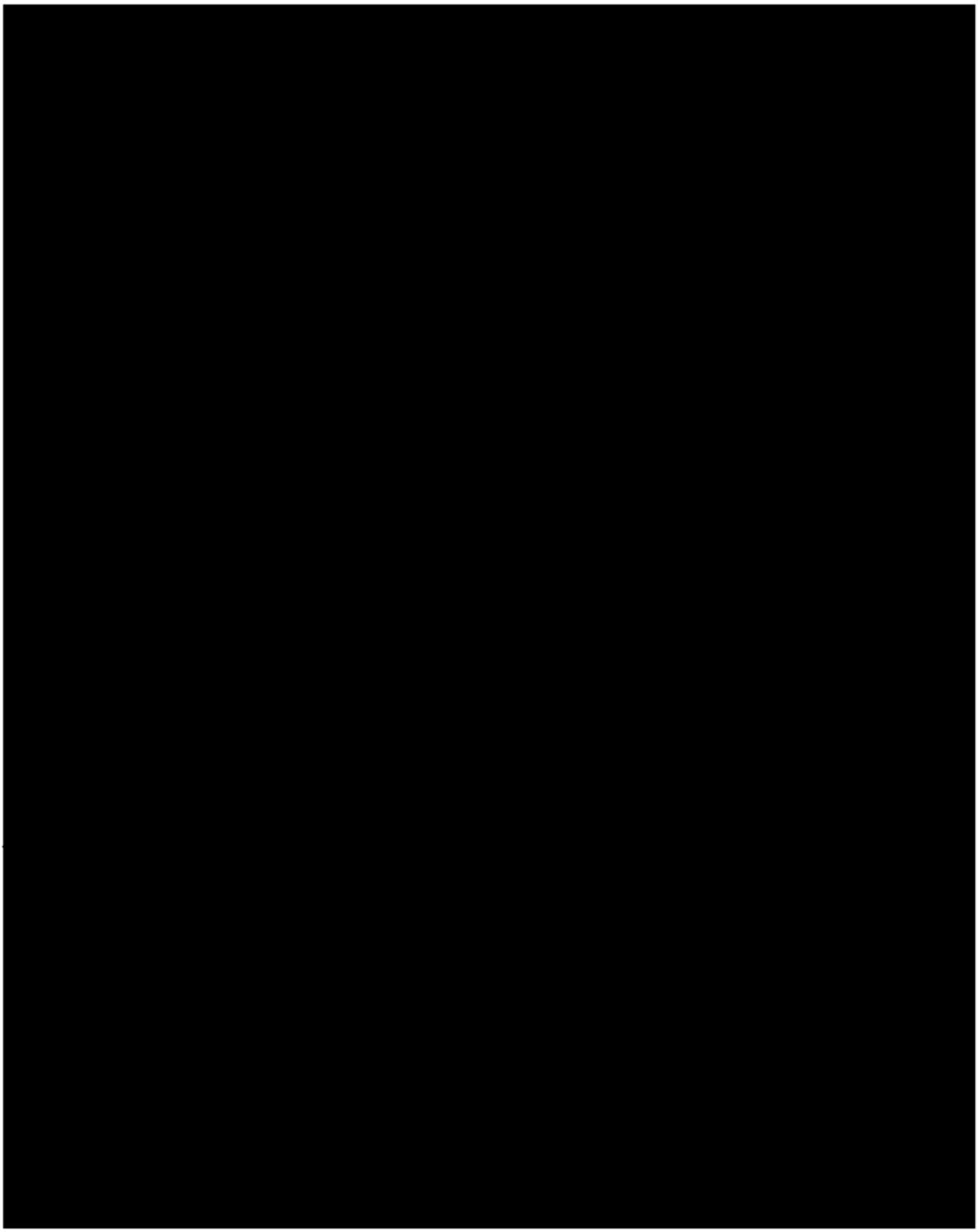

Q4
12
11
10
9

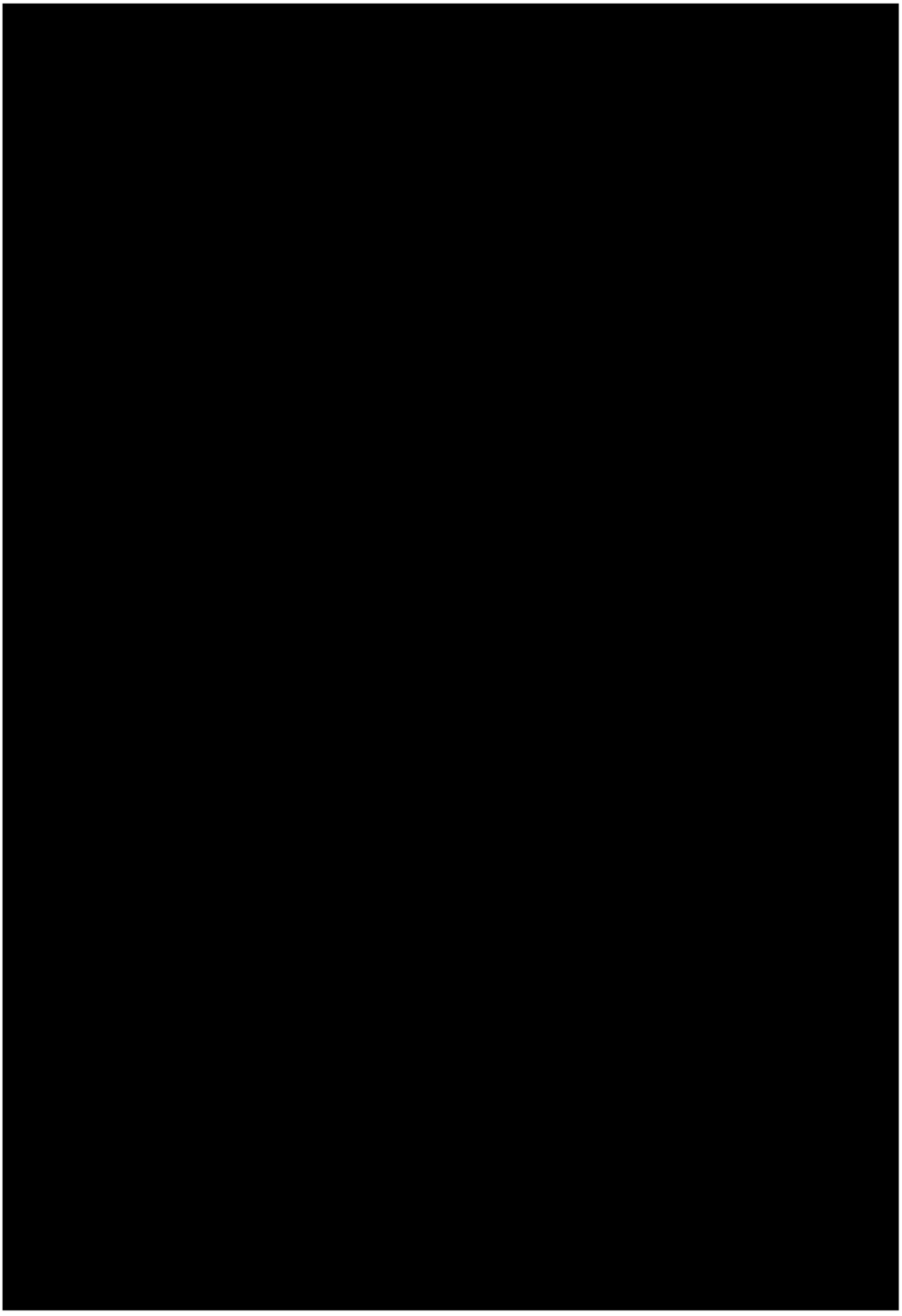


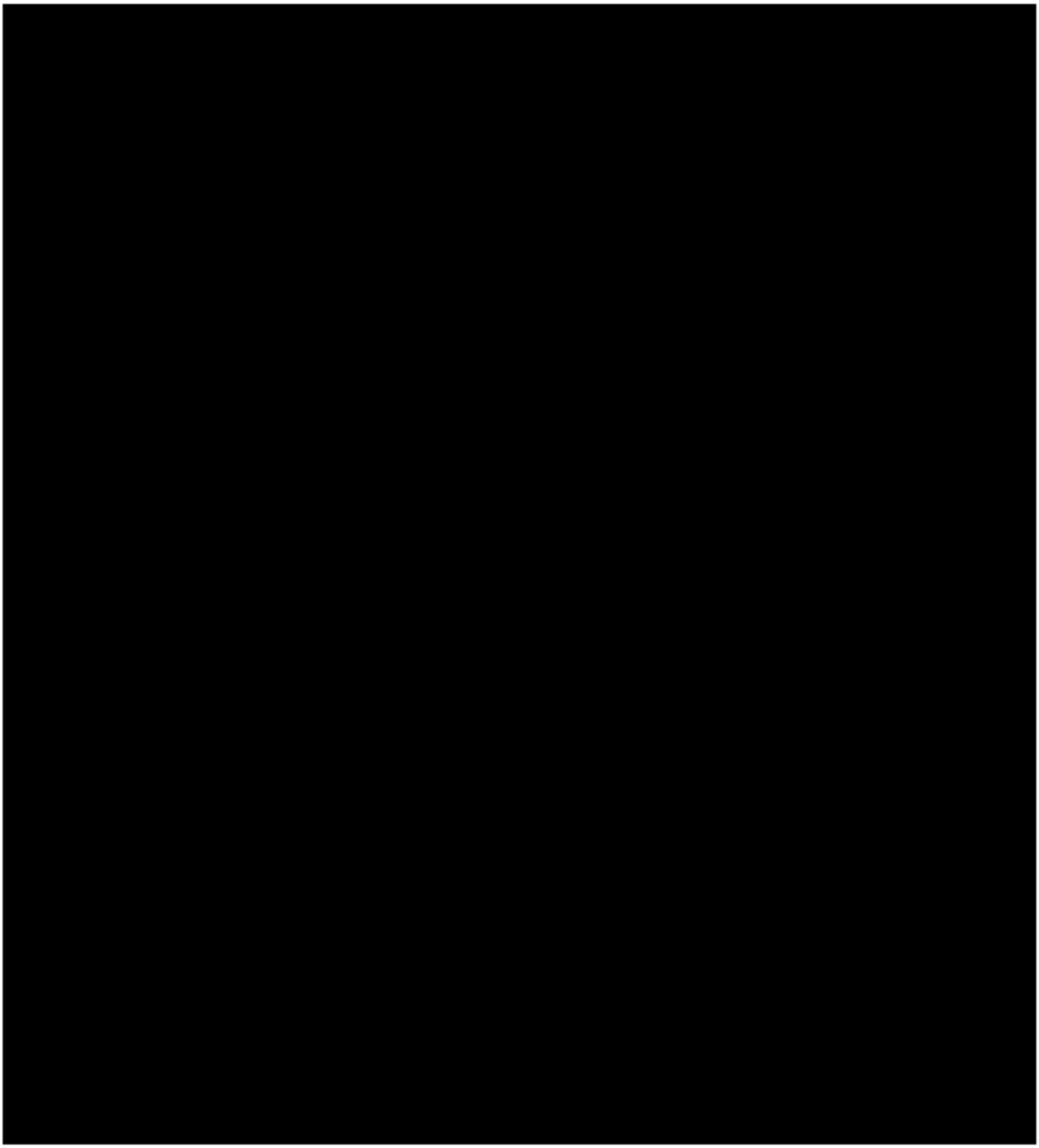


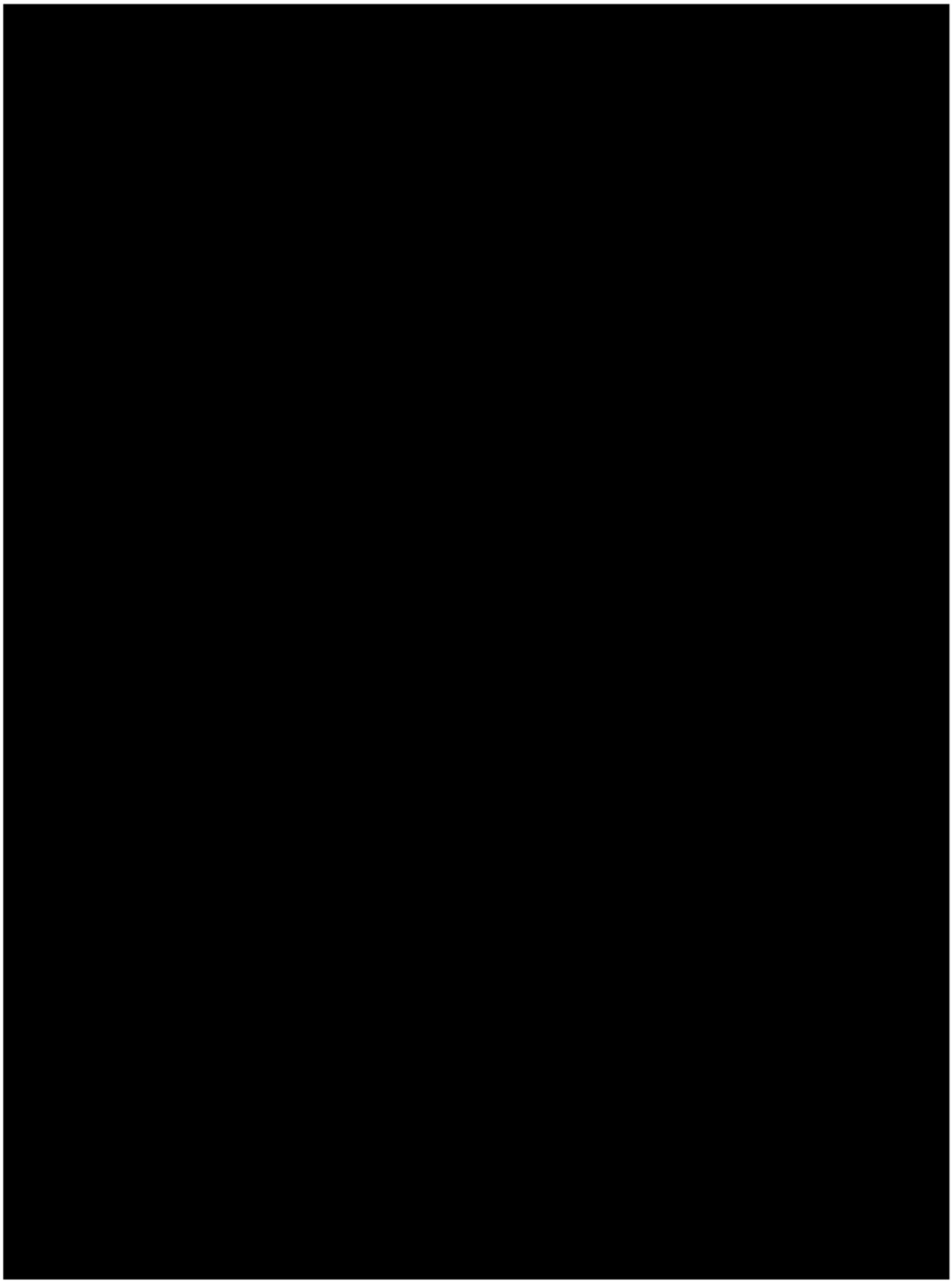


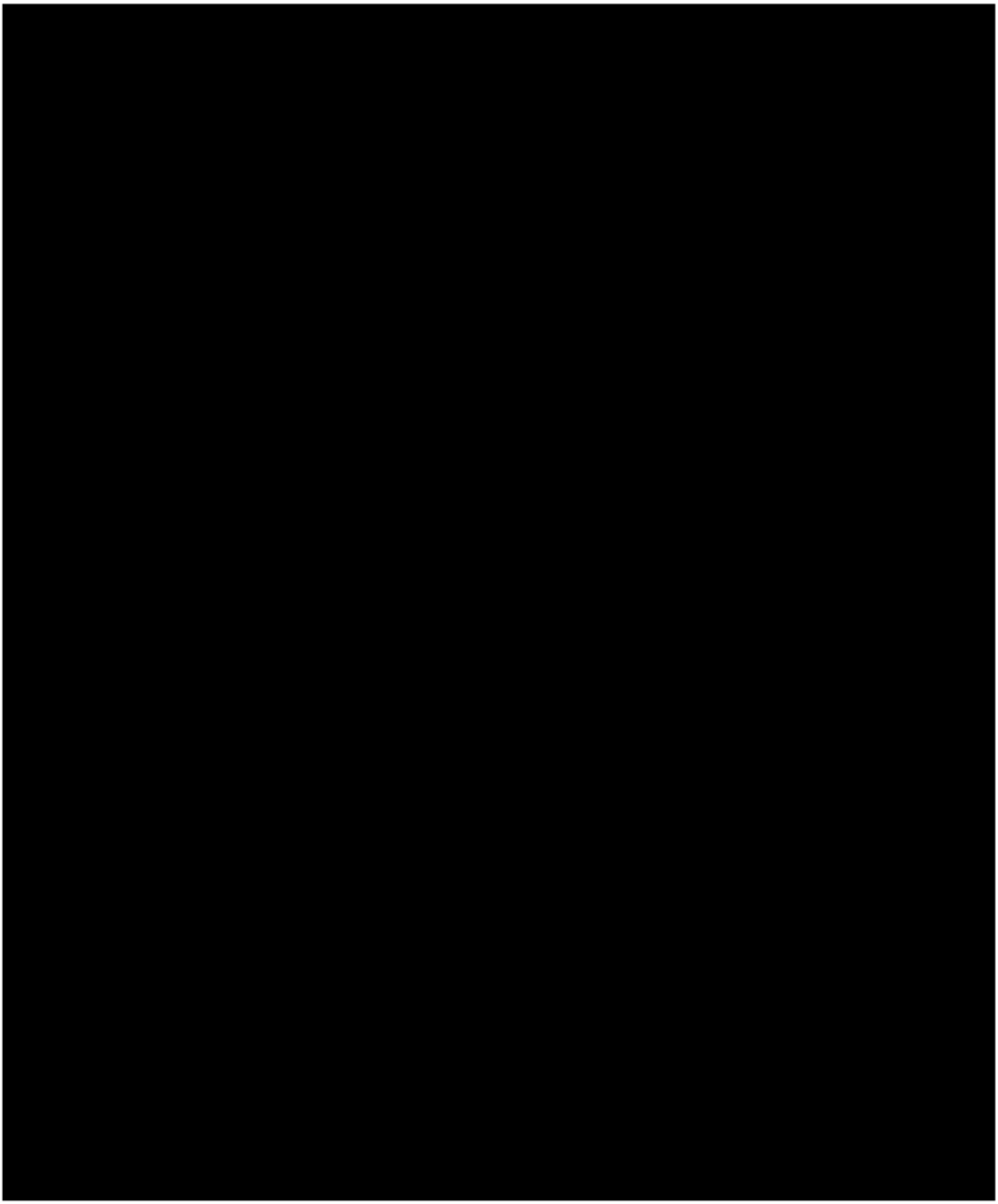


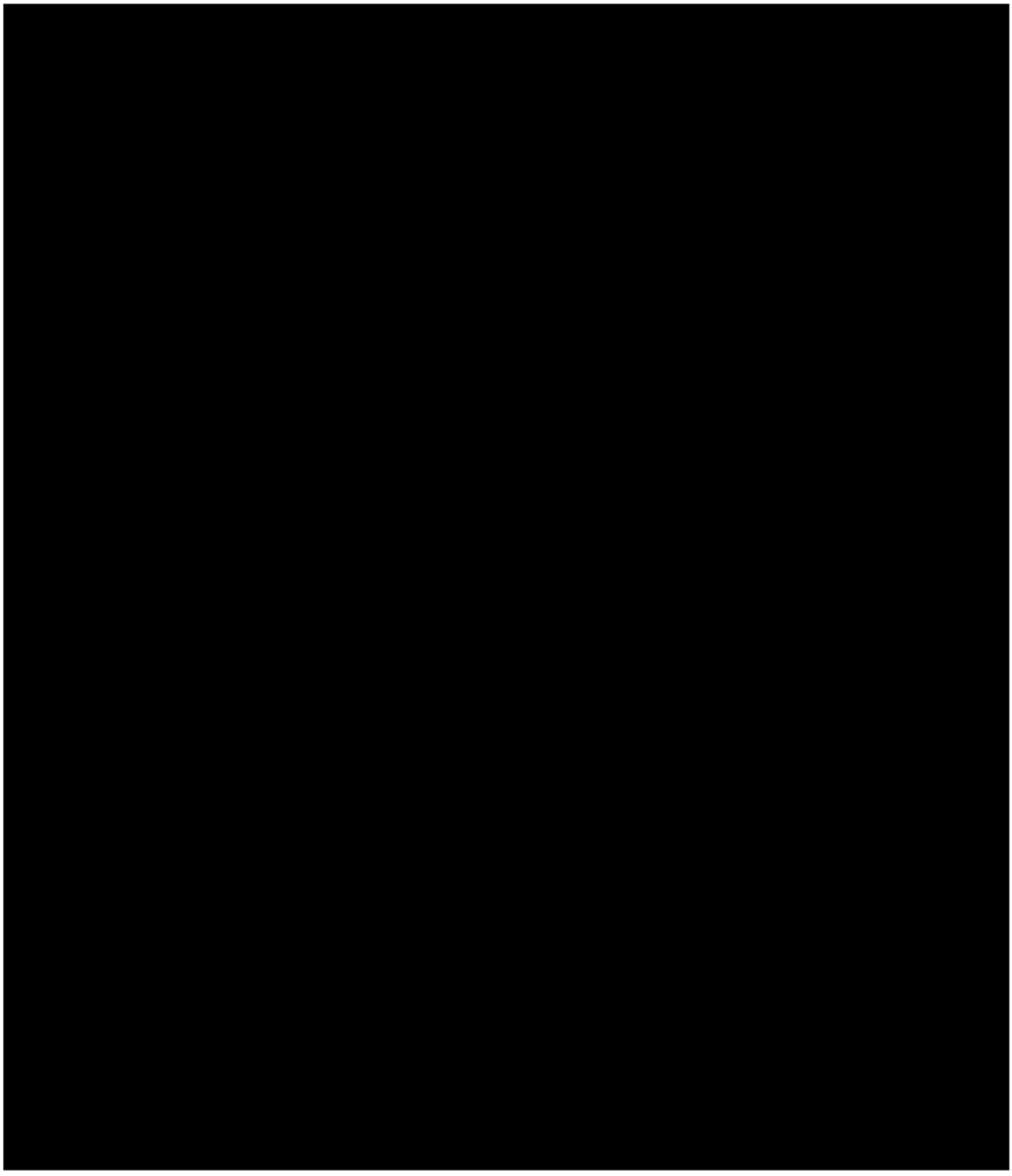


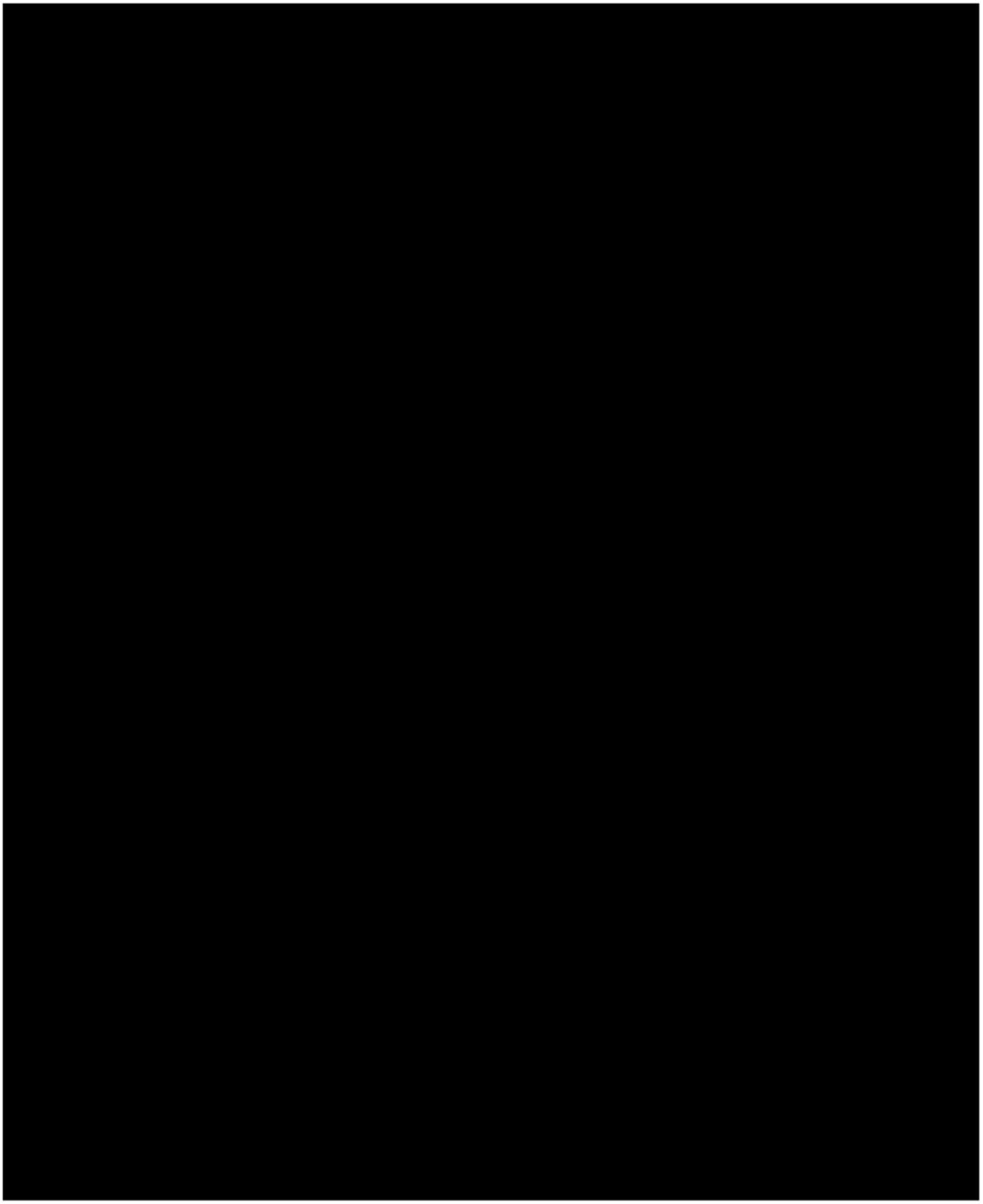


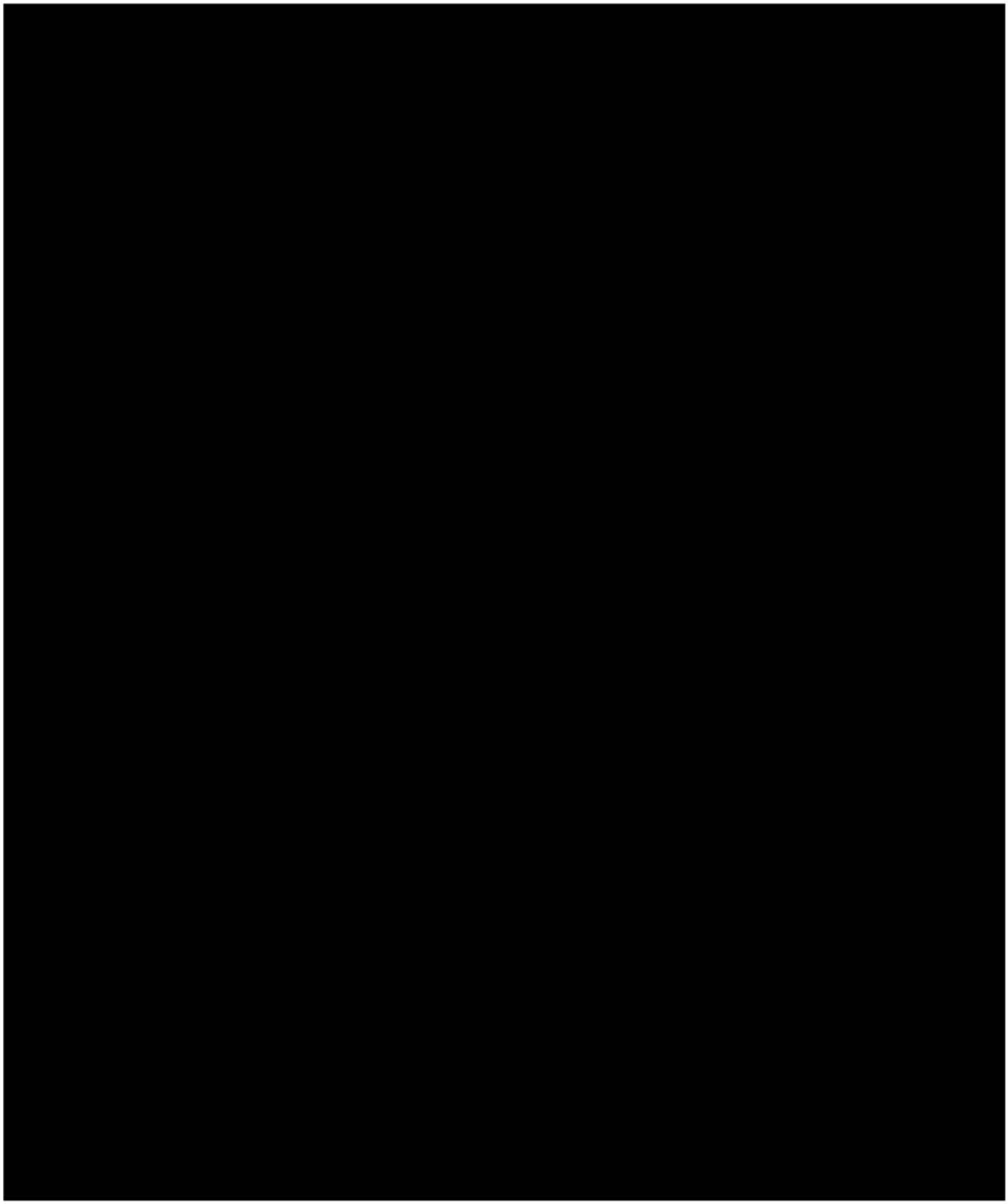


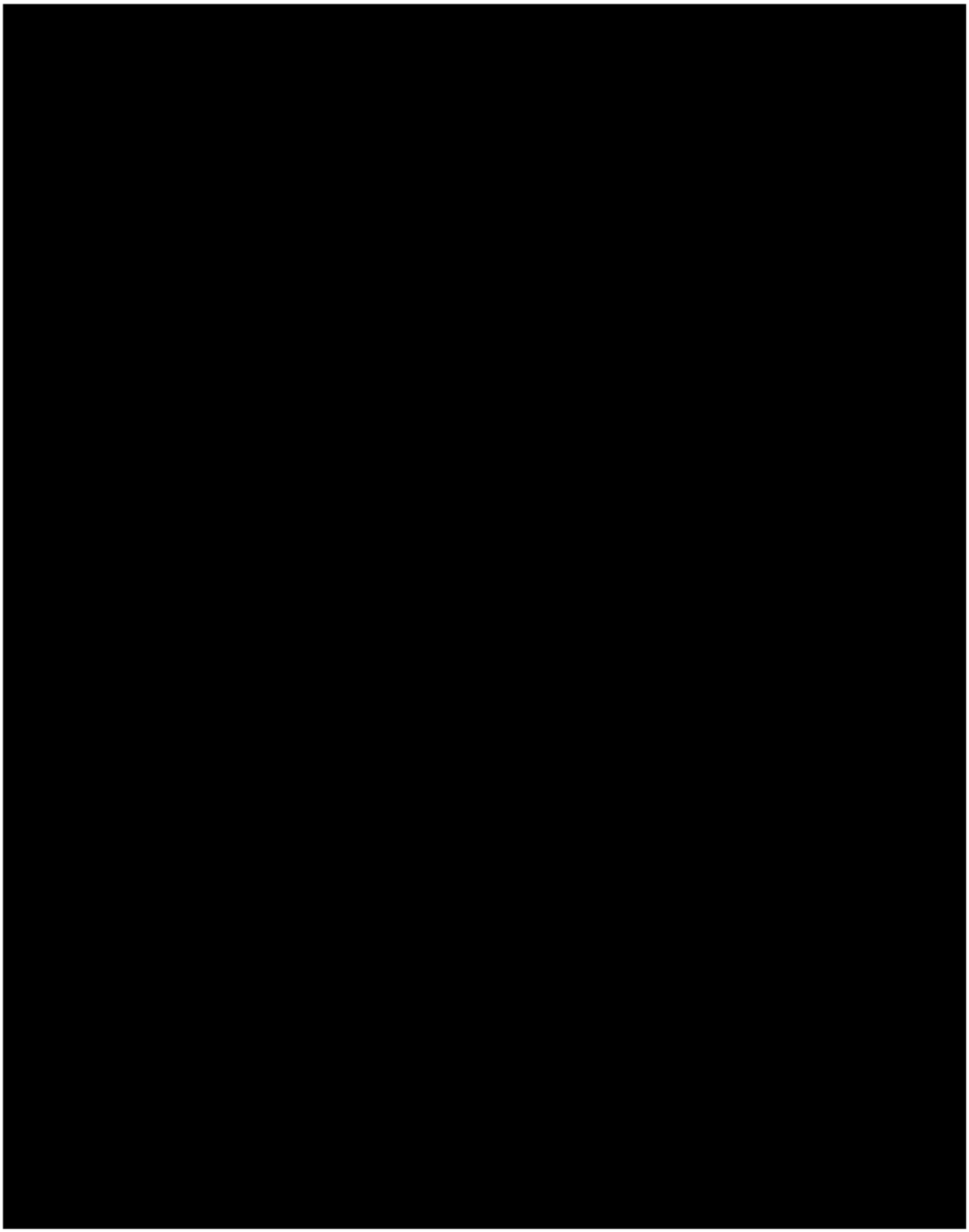




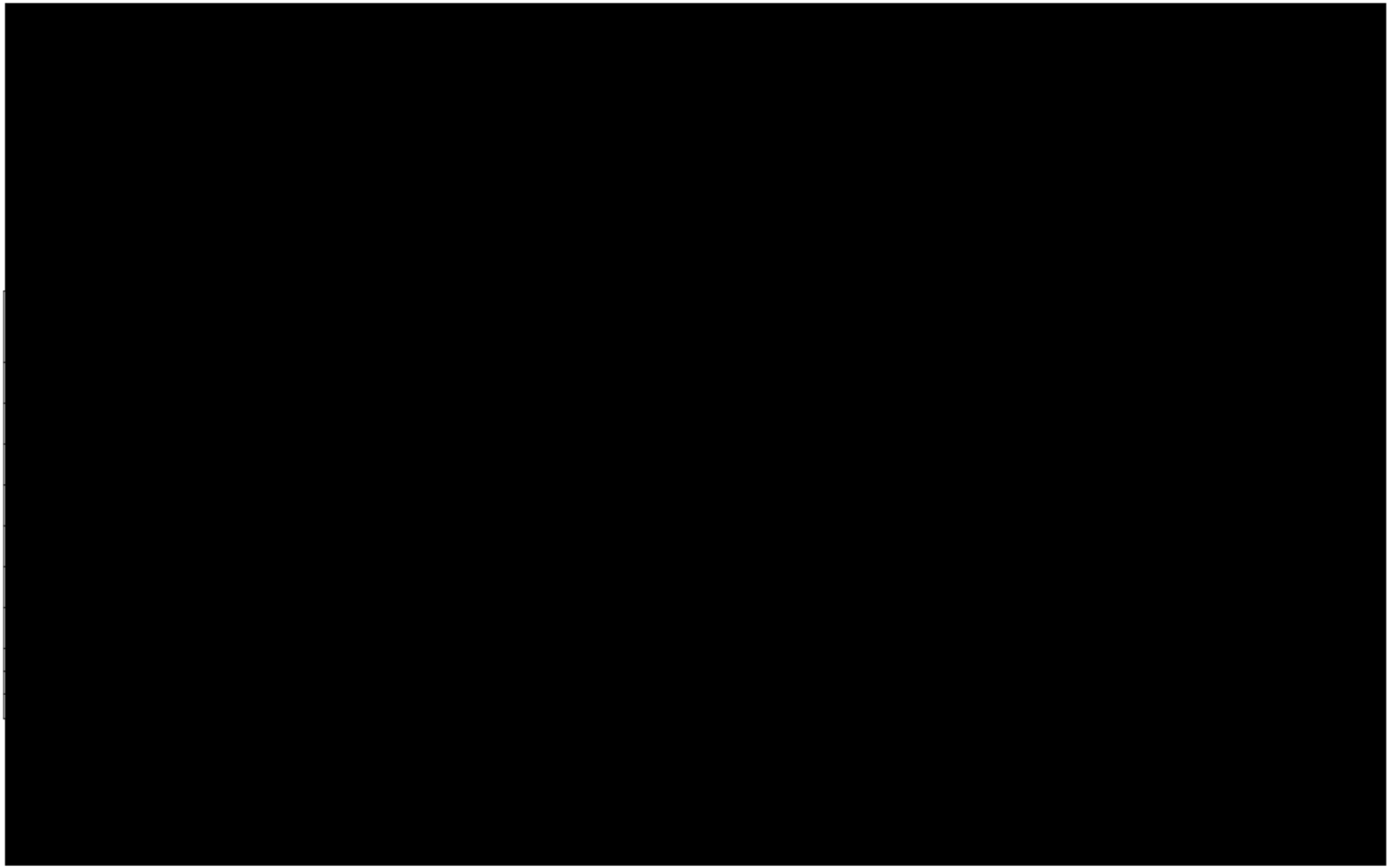


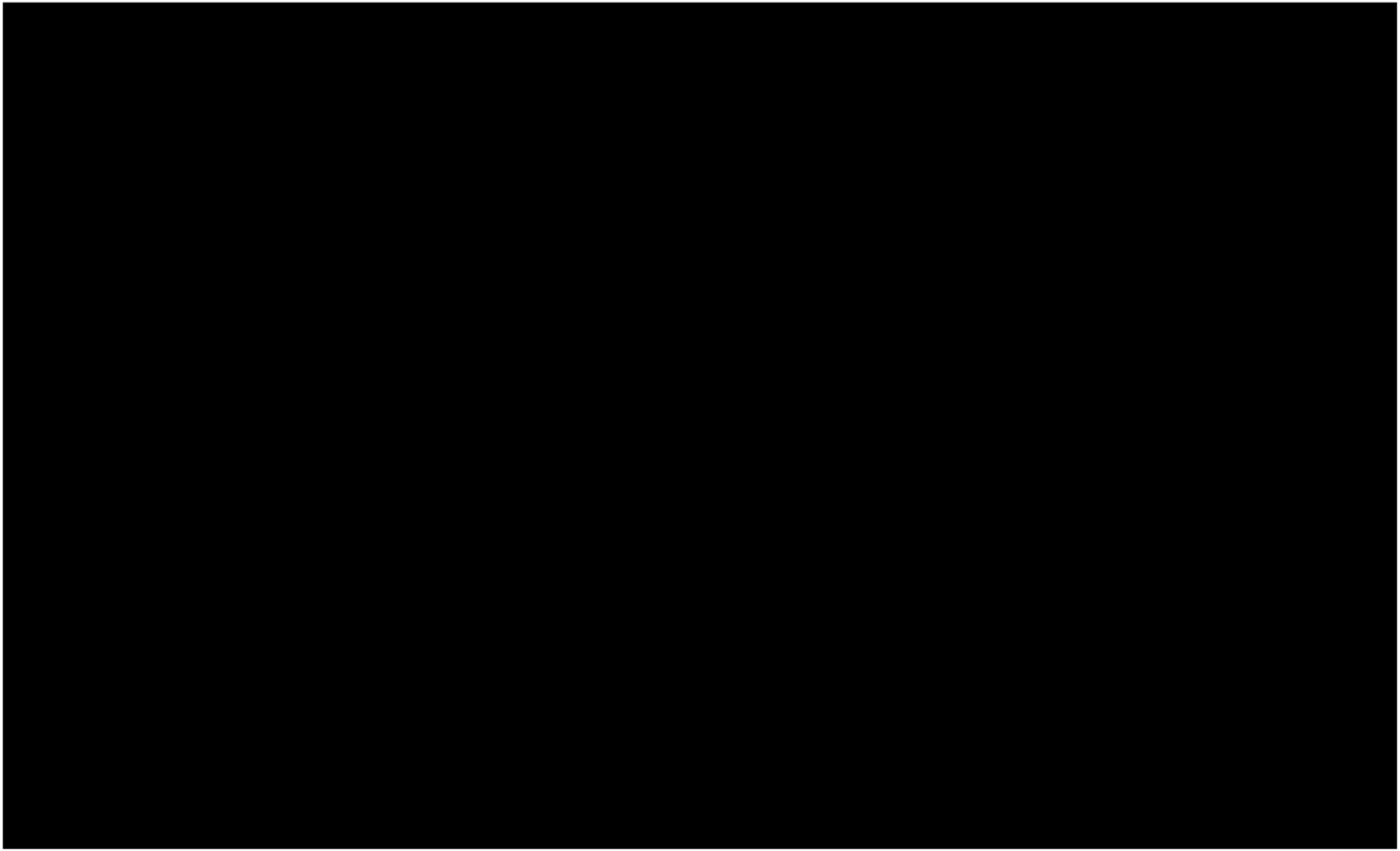






[11] Náv
navrho
podpoi





Příloha č. 3 ke smlouvě č. 2201 5 7370
Počet stran: 8

Takticko-technické požadavky projektu obranného vývoje

„CYBERTHREATS – Využití umělé inteligence při obraně proti kybernetickým útokům“

Praha 2022

Obsah

1. Identifikace vojenského materiálu

1.1 Úplný název vyvíjeného vojenského materiálu

„CYBERTHREATS – Využití umělé inteligence při obraně proti kybernetickým útokům“

1.2 Návrh zkráceného názvu

CYBERTHREATS

1.3 Určení a základní charakteristika

Cílem projektu je vyvinout a zavést do používání prototyp systému nástrojů detekce nasaditelných do síťového prostředí (dále „Systém“). Ten bude sloužit k monitoringu síťového provozu v koncových i vysokorychlostních transportních sítích (dále jen „infrastruktura“) a detekovat pokusy o kompromitaci zařízení v síti pomocí rozšířené analýzy a anotace šifrovaných dat pomocí postranních kanálů (dále jen „anotace“) odhalovat již kompromitovaná zařízení. Aby byla zajištěna detekce událostí na strategické úrovni, bude Systém získávat informace z centrálního úložiště, kde se budou shromažďovat data ze všech Systémů. Systém bude nad těmito daty provádět analýzu a korelaci událostí a následně obohacená data vracet zpět k dalšímu využití.

V současné době na trhu neexistuje plně funkční a komplexní řešení pro obranu kybernetického prostoru státu velikosti České republiky, které by bylo možné nasadit do koncových sítí i do infrastruktury a zároveň by široce spoléhalo na vyhodnocování pomocí umělé inteligence. Několik firem nabízí řešení využití umělé inteligence pro detekci kompromitace zařízení v podnikové síti, nebo detekci škodlivého síťového provozu v infrastruktuře. Podnikové sítě jsou svým způsobem připojení pouze koncové a nasazení komerčních zařízení do těchto sítí nepočítá s nasazením v infrastruktuře a korelacemi událostí napříč Systémy v různých místech nasazení. Komerční řešení pro infrastrukturu stále ve velké míře spoléhá na práci velkého množství analytiků. Žádný z veřejně známých projektů také není vyvíjen prioritně pro účely bezpečnosti a obrany České republiky. Z tohoto důvodu je nutné podobný systém vyvinout. Zároveň není vhodné tento Systém zabezpečit akvizicí od jiného, byť i partnerského státu, neboť by tím byl ohrožen hlavní cíl projektu, a to je získání operační výhody rezortu Ministerstva obrany České republiky v této oblasti.

Jedná se o novou technologii, která není v rámci Ministerstva obrany doposud zavedena. V rámci rozvoje schopností Ministerstva obrany přinese tato technologie zcela nové možnosti a napomůže výrazně rozvinout schopnosti a získat operační výhodu v oblasti kybernetických operací. Vývoj samotný má přesah do spousty dalších technických i netechnických oborů. Po ukončení vývoje existuje velký potenciál pro další rozvoj technologie ve všech odvětvích kybernetických operací i mimo ně. Požadovaná technologie je v současné době široce zkoumána a zaváděna ve všech odvětvích lidských činností napříč všemi vyspělými zeměmi.

V rámci Ministerstva obrany se vytváří nové schopnosti v oblasti kybernetických operací. Neustálý nárůst množství šifrovaného provozu na síti a absence nástrojů pro jejich analýzu a anotaci snižuje bezpečnost a obranyschopnost státu. Díky nárůstu šifrovaného provozu vzniká potenciální hrozba, kterou by měl navrhovaný Systém adresovat. Systém výrazně zlepší možnosti průzkumu a obrany v kybernetickém prostoru a také značnou měrou přispěje ke schopnostem České republiky reagovat na nenadálé situace ohrožující bezpečnost státu ať už vojenského nebo civilního charakteru. V případě nasazení na území České republiky budou síťová data ze Systému klíčovým zdrojem zpravodajských informací o potenciálních útočnících, neboť skrze infrastrukturu České republiky protékají data států celé Evropy, které mohou přispět k zajištění strategické výhody a bezpečnosti.

1.4 Stupeň utajení technického zařízení a způsob manipulace s ním

TTP nejsou utajovány ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Předávat informace organizacím a osobám, které se na realizaci nepodílejí je možné jen se souhlasem zadavatele a příjemce podpory s výjimkou informací již veřejně publikovaných.

1.5 Rozsah platnosti takticko-technických požadavků

Takticko-technické požadavky Systému, specifikované v tomto dokumentu platí jako základní kritéria pro vývoj a mohou být upravovány na základě společného jednání mezi zadavatelem a příjemcem podpory, na základě nových trendů v oblasti technického a technologického vývoje.

1.6 Požadavky na hodnocení plnění takticko-technických požadavků

Ověření kvalitativních parametrů Systému a požadavků na něj kladených těmito TTP v procesu jednotlivých etap vývoje bude ověřovat zadavatel v součinnosti s příjemcem podpory.

O provedení zkoušek zpracovat písemnou zprávu o provedených dílčích zkouškách, prohlášení, stanoviska, vyjádření apod. Výsledky zprávy projednat se zástupci příjemce podpory.

Hodnocení bude obsahovat výsledky zkoušek požadovaných schopností v oblasti detekce hrozeb, anotace šifrovaného provozu, spolehlivosti Systému.

Hodnocení jednotlivých etap vývoje bude posuzováno zkušební komisí z pohledu shody předložené dokumentace, takticko-technických parametrů se smluvně stanovenými parametry a požadavky. V případě shody, kdy zkušební komise vyhodnotí zkoušky jako „vyhovující“, bude projekt pokračovat další etapou. V případě identifikované neshody, kdy zkušební komise vyhodnotí zkoušky jako „nevyhovující“ bude požadována náprava a doplnění identifikovaných nedostatků ve vzájemně dohodnutém termínu.

2. Požadavky na základní taktické vlastnosti a funkce

2.1 Požadavky na výkonové, rozměrové a hmotnostní parametry

2.1.1 Návrh HW

Systém se bude skládat z hardwarových zařízení a softwarových části, které budou zajišťovat akvizici dat ze sítě, jejich zpracování a vyhodnocování a komunikaci se systémem IBM QRadar. Zpracování zachycených síťových dat bude využívat kromě analýzy a anotace šifrovaných síťových dat také IDS systém Suricata. Hardwarová zařízení budou navržena tak, aby bylo možné dosáhnout požadované přenosové rychlosti od 100 Mb/s až do 100 Gb/s. Pro konstrukci hardwarových zařízení bude využito dostupných serverových platforem. Výběr platformy zajistí zpracovatel s ohledem na požadované parametry Systému. Pro akvizici dat ve vysokorychlostních sítích bude využita technologie akcelerovaných síťových karet FPGA. Díky technologii FPGA bude také možné přesunout časově kritické operace do akcelerační karty, a tím zvyšovat výkonnost systému k požadované přenosové rychlosti.

Požadovaný hardware se velikostí může lišit dle množství použitých technologií řešitele, ale jednotlivé součásti hardwarové sestavy musí být kompatibilní s rackovými skříněmi podle EIA-310.

2.1.2 Návrh SW

Vytvořený software bude tvořen souborem bezpečnostních detektorů schopných provádět analýzu dostupných informací za účelem nalezení identifikátorů kompromitace zařízení v síti, šíření malware a dalších aktivit souvisejících s bezpečnostními hrozbami. Dodaný software musí být kompatibilní se SIEM systémem IBM QRadar. Software bude tvořen rozšiřujícími moduly, které budou přímo integrované do systému IBM QRadar a detekčními nástroji, které budou využívat IBM QRadar API pro přístup k uloženým informacích v systému. Detekční nástroje budou poskytovat výsledky v téměř reálném čase s ohledem na dostupnost dat v systému IBM QRadar. Výsledky budou prezentovány pomocí nových obrazovek vytvořených v systému IBM QRadar. Datové sady pro trénování a testování detektorů umělé inteligence jsou nezbytné pro vytvoření výsledků vyžadovaných dle kapitoly 1.6, ale bude je možné také použít samostatně pro výzkum a vývoj dalších detekčních metod. Software bude realizován pomocí vhodných softwarových technologií a nástrojů vzhledem k řešení projektu. Jejich výběr je omezen pouze s ohledem na licenci a požadavků plynoucích z integrace se systémem IBM QRadar. Je požadováno předání zdrojového kódu k softwaru, včetně licence k použitému softwaru.

2.1.3 Technické parametry zařízení

Takticko-technické požadavky Systému, specifikované v tomto dokumentu platí jako základní kritéria pro vývoj a mohou být upravovány na základě společného jednání mezi zadavatelem a příjemcem podpory, na základě nových trendů v oblasti technického a technologického vývoje.

Prototyp musí splňovat požadavky legislativních dokumentů, norem a předpisů uvedených v příloze č. 3 TTP.

2.1.4 Etapy vývoje

Projekt bude vyvíjen v následujících etapách

- Etapa 1: Oponentní řízení k předběžnému projektu;

- Etapa 2: Oponentní řízení ke konečnému projektu;
- Etapa 3: Vytvoření základního prototypového řešení (demo);
- Etapa 4: Stabilní verze prototypového řešení;
- Etapa 5: Zpracování průvodní a provozní dokumentace prototypu;
- Etapa 6: Pilotní testování příjemcem podpory a prezentace výsledků;
- Etapa 7: Podnikové zkoušky a úprava po podnikových zkouškách;
- Etapa 8: Kontrolní a schvalovací zkoušky a úprava prototypu po podnikových zkouškách;
- Etapa 9: Úprava dokumentace po provedených zkouškách a úpravách prototypu;
- Etapa 10: Zpracování závěrečné zprávy projektu obraného vývoje;
- Etapa 11: Závěrečné oponentní řízení;
- Etapa 12: Odevzdání výsledků vývoje;

2.2 Požadavky na přepravitelnost a manipulovatelnost

Prototyp musí splňovat podmínku na přepravitelnost běžnými prostředky zavedenými v rámci Ministerstva obrany.

2.3 Požadavky na vybavení softwarem

Systém bude vybaven softwarem, který je specifikován v kapitole 2.1.2.

2.4 Požadavky na komunikační a informační slučitelnost

Požadujeme, aby součástí dodaného systému byla sada zásuvných modulů do systému IBM QRadar SIEM, které budou poskytovat:

- vstup dat z nástroje detekce do systému QRadar,
- detekci bezpečnostních incidentů pro nové události z databáze uložených událostí,
- vizuální pohled na síťová data, obsahující anotaci šifrovaného provozu.

2.5 Požadavky na životnost

Životnost:

- životnost (doba životního cyklu) min. 10 let
- doba používání (celková životnost) do celkové repase (hardware) min. 5 let

2.6 Požadavky na provoz a obsluhu

Systém uvedený do provozu je koncipován jako bezobslužný v případě bezproblémového fungování v místě nasazení. Obsluha Systému bude vyškolena v rámci předávání prototypu.

3. Technické požadavky

3.1 Požadavky na objekt zástavby

Systém musí splňovat požadavky legislativních dokumentů, norem a předpisů uvedených v příloze č. 3 TTP.

3.2 Požadavky na elektronickou, elektromagnetickou a další typy ochran

Bez požadavků.

3.3 Požadavky na stálost, pevnost a odolnost proti působení mechanických vlivů

Bez požadavků.

3.4 Požadavky na elektrické napájení

Požaduje se použití hardwarové platformy s možností využití redundantního zdroj energie pro zajištění nepřetržitého chodu i v případě poruchy primárního napájecího zdroje.

3.5 Požadavky na preventivní údržbu, opravy, meteorologické zabezpečení a podporu (včetně požadavků na revize a zkoušky určených technických zařízení)

Požaduje se, aby konstrukce jednotlivých částí Systému umožnila provádění preventivní údržby v systému zavedeném v rámci Ministerstva obrany v rozsahu:

- kontrolní prohlídka;
- zvláštní druhy údržby;
- zákonné revize vybraných (určených) technických zařízení.

3.6 Požadavky na bezpečnost (včetně požární a určených technických zařízení)

Požaduje se, aby všechny segmenty Systému a všechny jeho díly plnily požadavky z hlediska bezpečnosti a ochrany zdraví při práci a při výkonu služby a požadavky předpisů požární ochrany.
Elektrická zařízení Systému musí být provedena v souladu s normami ČSN 33 2000-4-41 a ČSN 33 1310.

3.7 Požadavky na hygienu a ochranu zdraví při práci s rizikovými faktory pracovních podmínek

Požaduje se, aby všechny segmenty Systému a všechny jeho díly plnily požadavky základních hygienických podmínek pro činnost osob stanovené příslušnými předpisy, plnily požadavky z hlediska bezpečnosti a ochrany zdraví při práci a při výkonu služby a požadavky předpisů požární ochrany.

3.8 Požadavky na spolehlivost

Klasifikace Systému:

- obnovovaná po poruše;
- provozní režim obecný;

Omezení doby používání:

- plánované technická údržba, zákonné revize;
- vynucené oprava z důvodu závady na systému.

Ukazatele spolehlivosti Systému:
Životnost:

- životnost (doba životního cyklu) min. 10 let

- doba používání (celkový život) do celkové repase (hardware) min. 5 let

U určených technických zařízení (ve smyslu vyhlášky MO č. 273/1999 Sb.), které podléhají zákonným revizím:

- doba revize elektrické instalace a elektrických zařízení 1 rok
- doba validace účelové výbavy a zařízení 1 rok

3.9 Specifické konstrukční a technologické požadavky

Bez požadavků.

3.10 Požadavky na instalaci a záruky

Softwarové vybavení je součástí příslušného přístrojového vybavení.

4. Ostatní požadavky

4.1 Požadavky na přihlášení k realizaci obraného projektu

Součástí přihlášky musí být studie proveditelnosti ze strany příjemce podpory.

4.2 Požadavky na balení a značení

Segmenty Systému musí být označeny štítkem výrobce.

4.3 Požadavky na dokumentaci

Průvodní a výrobní dokumentaci Systému se požaduje zpracovat dle platného RMO 1/2017, ČOS 051632 v rozsahu:

- Seznam předmětů Systému;
- Příručka pro obsluhu Systému;
- Návody pro obsluhu Systému;
- Průvodní doklady o kvalitě zhotoveného výrobku;
- Zápisy o odborných prohlídkách a zkouškách určených technických zařízení (zprávy o výchozí revizi, karty revizí a kontrol elektrických spotřebičů podle ČSN 33 1610 apod.);
- Výrobní dokumentace prototypu CYBERTHREATS.

4.4 Ekologické požadavky

Z hlediska ochrany životního prostředí před nepříznivými účinky elektromagnetického záření vznikajících při chodu Systému se požaduje vybavit jej odpovídajícími technickými prostředky, pomůckami a materiály.

4.5 Požadavky na likvidaci

Běžný provoz Systému nesmí ohrožovat životní prostředí a likvidace výrobku musí být řešena v souladu se zákonem č. 185/2001 Sb., o odpadech a s vyhláškou č. 38/2016 Sb., katalog odpadů, ve které jsou roztříděny odpady podle nebezpečnosti pro životní prostředí.

4.6 Požadavky na katalogizaci

Bez požadavků.

4.7 Ostatní jiné nespecifikované požadavky

Bez požadavků.

Příloha č. 4 ke smlouvě č. 2201 5 7370
Počet stran: 5

Charakteristika projektu obranného experimentálního vývoje

Program:	**907 050 – Ambice – podpora rozvoje oblastí, ve kterých ozbrojené složky dosahují významných výsledků v rámci NATO a EU**

Název projektu experimentálního vývoje:

„CYBERTHREATS - Využití umělé inteligence při obraně proti kybernetickým útokům“

Které konkrétní cíle (2. až 4. úrovně) Soustavy cílů rezortu MO na roky 2015–2022 projekt naplňuje:	4. zajištění strategického zpravodajství		
Manažer cíle:	Ředitel vojenského zpravodajství		
Které konkrétní cíle a priority programu **907 050** projekt naplňuje:	**Rozvoj systémů velení a řízení, komunikačních a informačních systémů a kybernetické obrany** - rozvíjet systémy určené pro podporu ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance)		
Priorita projektu:	Střední		
Rok zahájení řešení projektu	2022	Rok ukončení řešení projektu	2025

Výsledek projektu (povinně označit nejméně jeden z uvedených)[1]

☐ P – patent
☑ G – technicky realizované výsledky – prototyp, funkční vzorek
☐ Z – poloprovoz, ověřená technologie
☐ R – software
☐ F – průmyslový a užitný vzor
☐ H – výsledky promítnuté do směrnic a předpisů (vnitřních předpisů)
☐ N – certifikované metodiky, léčebné postupy, specializované mapy

Konkrétním výsledkem projektu uvedeným ve smlouvě bude: Prototyp modulárního expertního systému na bázi umělé inteligence pro analýzu síťových dat, výrobní dokumentace a software prototypu.

Stupeň utajení výsledků projektu[2]	**Bezpečnostní důstojník (v případě volby V, D, T, PT) – uveďte kontakt na bezpečnostního důstojníka projektu**
☑ **neutajované (O)** ☐ **vyhrazené (V)** ☐ **důvěrné (D)** ☐ **tajné (T)** ☐ **přísně tajné (PT)**	

Cíl (cíle) projektu a popis konkrétních požadovaných výsledků a výstupů, které budou převzaty uživatelem – čeho má být řešením projektu dosaženo.

[1] Jeden ze znaků ☑☐ vymažte

Cílem projektu je vyvinout a zavést do používání prototyp systému nástrojů detekce nasaditelných do síťového prostředí (dále „Systém“). Ten bude sloužit k monitoringu síťového provozu v koncových i vysokorychlostních transportních sítích (dále jen „infrastruktura“) a detekovat pokusy o kompromitaci zařízení v síti pomocí rozšířené analýzy a anotace šifrovaných dat pomocí postranních kanálů (dále jen „anotace“) odhalovat již kompromitovaná zařízení. Aby byla zajištěna detekce událostí na strategické úrovni, bude Systém získávat informace z centrálního úložiště, kde se budou shromažďovat data ze všech Systémů. Systém bude nad těmito daty provádět analýzu a korelaci událostí a následně obohacená data vracet zpět k dalšímu využití.

Systém se bude skládat z hardwarových zařízení s rychlostí linek až 100Gb/s a softwarových částí, které budou zajišťovat komunikaci, akvizici dat ze sítě, jejich zpracování, vyhodnocení a prezentaci. Hardwarová zařízení budou na existující serverové platformě dle návrhu zpracovatele. Pro akvizici dat v infrastruktuře sítích bude využita technologie akcelerovaných síťových karet (dále jen „FPGA“). Softwarová část zajišťující komunikaci mezi Systémem a centrálním úložištěm dat musí být kompatibilní se systémem IBM QRadar SIEM.

Součástí vývoje bude školení vybraného personálu v manipulaci se systémem – konfigurace, uvedení do provozu, příjem a zpracování dat a procedury nutné pro provoz Systému.

Hlavní přínosy využití předpokládaných výsledků vzhledem k současnému stavu:

Komunikační síť se neustále vyvíjí a zrychluje a není v lidských silách zajistit nepřetržité sledování a analýzu přenášeného datového toku. Přímou úměrou k neustále se zvyšující rychlosti je množství dat, které tímto vzniká a jejich následná analýza vyžaduje nepoměrně více lidského úsilí a času. Z toho důvodu je vhodné k analýze a anotaci šifrovaného provozu využít umělou inteligenci, která z velkého množství dat může při svém nasazení těžit a díky pokročilým algoritmům je schopná najít souvislosti v datech lépe než člověk. Při objevení již probíhající kompromitace je schopna se rychle podívat do minulosti, pokud jsou data pro daný segment k dispozici, a objevit v nich komunikační vzorce, které ke kompromitaci vedly, tím pomoci při atribuci útočníka a na základě získaných dat předpokládat jeho další kroky. K nasazení Systému do infrastruktury je nutné využití technologie FPGA, na kterou celý tento síťový segment spoléhá. V budoucnosti bude tato technologie stále více využívaná, což bude výhoda pro vyškolenou obsluhu, která bude již mít praktické zkušenosti a tím získá technologický náskok. Předpokladem udržitelnosti tohoto projektu je kontinuální vývoj a zlepšování detekčních i predikčních schopností Systému s rozvojem umělé inteligence a zvyšováním množství dat v síti. Znalosti a zkušenosti získané z tohoto projektu, bude možné aplikovat i v dalších odvětvích mimo oblast kybernetických operací.

Širší kontext řešení projektu – hlavní odlišnosti požadovaného řešení od současného stavu, známé způsoby řešení v ČR a v zahraničí. Zdůvodnění preference vlastního vývoje před jiným možným řešením (např. akvizicí).

V současné době na trhu neexistuje plně funkční a komplexní řešení pro obranu kybernetického prostoru státu velikosti České republiky, které by bylo možné nasadit do koncových sítí i do infrastruktury a zároveň by široce spoléhalo na vyhodnocování pomocí umělé inteligence. Několik firem nabízí řešení využití umělé inteligence pro detekci kompromitace zařízení v podnikové síti, nebo detekci škodlivého síťového provozu v infrastruktuře. Podnikové sítě jsou svým způsobem připojení pouze koncové a nasazení komerčních zařízení do těchto sítí nepočítá s nasazením v infrastruktuře a korelacemi událostí napříč Systémy v různých místech nasazení. Komerční řešení pro infrastrukturu stále ve velké míře spoléhá na práci velkého množství analytiků. Žádný z veřejně známých projektů také není vyvíjen prioritně pro účely bezpečnosti a obrany České republiky. Z tohoto důvodu je nutné podobný systém vyvinout. **Zároveň není vhodné tento Systém zabezpečit akvizicí od jiného, byť i partnerského státu, neboť by tím byl ohrožen hlavní cíl projektu, a to je získání operační výhody rezortu Ministerstva obrany České republiky v této oblasti.**

Jakým způsobem výsledek projektu podpoří dlouhodobou strategii a cíle MO, která cílová schopnost organizačního celku rezortu bude udržována nebo rozvíjena po skončení řešení projektu. Uvedení návaznosti projektu na střednědobý plán rozvoje MO.

Jedná se o novou technologii, která není v rámci Ministerstva obrany doposud zavedena. V rámci rozvoje schopností Ministerstva obrany přinese tato technologie zcela nové možnosti a napomůže výrazně rozvinout schopnosti a získat operační výhodu v oblasti kybernetických operací. Vývoj samotný má přesah do spousty dalších technických i netechnických oborů. Po ukončení vývoje existuje velký potenciál pro další rozvoj technologie ve všech odvětvích kybernetických operací i mimo ně. Požadovaná technologie je v současné době široce zkoumána a zaváděna ve všech odvětvích lidských činností napříč všemi vyspělými zeměmi.

Zdůvodnění nezbytnosti realizace projektu. Začlenění výsledků projektu do zamýšleného (operačního) použití – které konkrétní aspekty z hlediska rozvoje schopností budou projektem vyřešeny.

V rámci Ministerstva obrany se vytváří nové schopnosti v oblasti kybernetických operací. Neustálý nárůst množství šifrovaného provozu na síti a absence nástrojů pro jejich analýzu a anotaci snižuje bezpečnost a obranyschopnost státu. Díky nárůstu šifrovaného provozu vzniká potenciální hrozba (viz příloha), kterou by měl navrhovaný Systém adresovat. Systém výrazně zlepší možnosti průzkumu a obrany v kybernetickém prostoru a také značnou měrou přispěje ke schopnostem České republiky reagovat na nenadálé situace ohrožující bezpečnost státu ať už vojenského nebo civilního charakteru. V případě nasazení na území České republiky budou síťová data ze Systému klíčovým zdrojem zpravodajských informací o potenciálních útočnících, neboť skrze infrastrukturu České republiky protékají data států celé Evropy, které mohou přispět k zajištění strategické výhody a bezpečnosti.

Uvedení veškerých nezbytných požadavků, které budou potřebné k realizaci přínosů projektu po jeho převzetí uživatelem.

Síťový provoz se neustále vyvíjí v čase, a to jak zastoupení různých typů komunikace, tak i skladba používaných komunikačních protokolů a jejich verzí. Zároveň se vyvíjí i kyberbezpečnostní hrozby, na které je potřeba reagovat. Proto je nutné uvažovat průběžnou aktualizaci vyvinutých algoritmů pro klasifikaci a detekci. Návrh projektu s touto skutečností počítá a pro minimalizaci stárnutí natrénovaných a otestovaných algoritmů vznikne sada nástrojů pro poloautomatické vytváření anotovaných trénovacích datových sad pro umělou inteligenci. Díky tomu se významně zjednoduší a urychlí zlepšování schopnosti Systému v průběhu řešení projektu a následně i po jeho dokončení. Tím bude zajištěna dlouhodobá udržitelnost a aktuálnost vyvinutých výstupů.

Možné negativní dopady (nevýhody) realizace výstupů projektu, které některá ze zainteresovaných stran vnímá negativně *(např. snížení výkonnosti složky v průběhu zavádění výstupů, redukce pracovních míst po zavedení výsledku do užívání apod.)*

Další negativní dopady nejsou známy.

Kritéria hodnocení naplnění cíle (cílů) projektu – způsob uplatnění výsledků při rozvíjení konkrétních schopností a cílů plánování činnosti a rozvoje MO. Určení kvantitativních a kvalitativních ukazatelů, které budou použity pro ověření změny schopností a přínosů, které má projekt přinést ve srovnání se současným stavem *(kritéria a ukazatele, podle kterých bude uživatel hodnotit přínos a intenzitu přínosu výsledků projektu poté, co mu budou předány (po dobu 5 let od jejich*

převzetí do užívání)).

Přesnost a rychlost vyhodnocování kybernetických hrozeb pro Českou republiku, s přesahem na sousední státy. Informační přehled v kybernetickém prostoru včetně prostoru mimo Českou republiku.

Analýza rizik:

- *výčet známých rizik včetně odhadu četnosti jejich vzniku (vysoká, střední, nízká)*
- *dopad rizik na realizaci výsledku a jeho následnou aplikovatelnost v resortu MO*

Nedodání požadovaného Systému by mohlo znamenat radikální zpomalení rozvoje schopnosti operovat v kybernetickém prostoru a tím i schopnost identifikovat případné bezpečnostních hrozby pro ČR.
Minimalizace rizika: Příjemce podpory musí mít mnoho zkušeností s úspěšným řešením výzkumných a vývojových projektů. Na základě těchto zkušeností jsou při výzkumu a vývoji využívány moderní nástroje a procesy řízení projektů. Během řešení projektu se počítá s intenzivní komunikací zadavatele s příjemcem podpory a průběžné předávání výsledků spolu se zapracováním zpětné vazby.

Dynamika síťového provozu, aktualizace komunikačních nástrojů a protokolů by mohlo znamenat zastarávání vyvinutých nástrojů, které nedokážou nový provoz anotovat.
Minimalizace rizika: Návrh projektu počítá s vytvořením systému (sady nástrojů) pro poloautomatické vytváření datových sad, což umožní rychle adaptovat vytvářené algoritmy postavené na technologiích umělé inteligence na nový typ provozu či hrozeb.

Objevení komunikačních nástrojů odolných proti analýze pomocí tzv. postranních kanálů, které by umožnily útočníkům skrývat jejich aktivity.
Minimalizace rizika: Cíle projektu jsou zaměřeny na analýzu provozu a detekci bezpečnostních hrozeb pomocí vyhodnocování charakteristik chování útočníka/aplikace a tím pádem výsledky nebudou závislé na konkrétním protokolu nebo jeho verzi.

Výrazný růst objemu síťového provozu může vést k neschopnosti zpracovat veškerou komunikaci.
Minimalizace rizika: Příjemce podpory musí mít zkušenosti s hardwarovou akcelerací, díky které je možné zpracovávat výrazně vyšší objemy síťového provozu než lze běžnými komoditními prostředky. Projekt cílí na schopnost zpracovávat provoz linek při dostatečně vysoké rychlosti linek tak, aby bylo dosaženo technologického náskoku.

Vstupy pro řešení projektu ~~jsou~~/nejsou vázány na práva duševního vlastnictví.

Pro řešení projektu ~~bude~~/nebude nutno použít techniku, či jiný materiál v užívání navrhovatele projektu.

Pro řešení projektu jsou/~~nejsou~~ ze strany příjemce (řešitele) nezbytné určité specifické znalosti a schopnosti *(např. zkušenosti z obranného výzkumu a vývoje, certifikace v určité oblasti, naplnění stupně utajení apod.).* **Jaké?**

Pro řešení projektu jsou ze strany příjemce podpory nezbytné specifické znalosti a schopnosti v oblasti vývoje informačních systémů, systémů pro distribuované výpočty, hardwarové akcelerace pro vysokorychlostní sítě, síťových komunikačních prostředků a navazujících oblastí k zajištění funkčnosti Systému. Vzhledem k výzkumné povaze projektu je nezbytností zkušenost s výzkumem a vývojem v oblasti síťové bezpečnosti a zpracování síťového provozu na vysokých rychlostech. Pro vytvoření použitelných výstupů, které bude možné nasadit do praxe a dlouhodobě provozovat, je dále důležitá zkušenost s provozováním infrastruktury monitorování síťového provozu a zpracování provozu za účelem

bezpečnostní analýzy.
Existují nějaká další omezení nebo specifické předpoklady pro řešení projektu a následné využití jeho výsledků? *(např. součinnost dalších složek AČR, rozhodnutí o následné akvizici a zabezpečení finančních prostředků apod.).* Zařadit do střednědobého plánu rozvoje Ministerstva obrany. Pro potřeby zadavatel vyčlení prostory k testování prototypu. Příjemce podpory musí být schopný pilotního provozu, a prezentace výsledků pilotního provozu, na vlastní infrastruktuře.
Plán následné akviziční činnosti – způsob, časový rámec a popis realizace nákupů (akvizic) – plánovaný počet následně pořizovaných výrobků a garance finančních prostředků na tuto návaznou akvizici *(týká se výsledku druhu prototyp).* Po dodání prototypu Systému bude požadováno zabezpečení dalších kusů. Akvizice bude zadána do akvizičního plánu. Vývojový projekt je potřeba realizovat co nejdříve, nejlépe od roku 2022 z důvodu prodlení nově nabývaných schopností v oblasti obrany před kybernetickými útoky a detekce síťových hrozeb.

Příloha č. 5 ke smlouvě č. 2201 5 7370
Počet stran: 1

KATALOGIZAČNÍ DOLOŽKA[1]

K zabezpečení procesu katalogizace položek majetku (výsledků výzkumu a vývoje), které jsou předmětem smlouvy a které podléhají katalogizaci podle zásad Kodifikačního systému NATO (dále jen „**NCS**") a Jednotného systému katalogizace majetku v ČR (dále jen „JSK") se **příjemce podpory** zavazuje:

1. Neprodleně po uzavření smlouvy, nejpozději do **5 pracovních dní**, oznámit e-mailem Oddělení katalogizace majetku Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti (dále jen „OdKM") na e-mailovou adresu [redacted] číslo smlouvy, kontaktní osobu a kontaktní údaje osoby zodpovědné ze strany příjemce podpory za provedení katalogizace položek dané smlouvy[2].
2. Na vlastní náklady zpracovat nebo zabezpečit zpracování Souboru povinných údajů pro katalogizaci (dále jen „SPÚK") majetku definovaného smlouvou vždy prostřednictvím aplikace umístěné na [redacted]
3. Povinnou součástí zpracování SPÚK každé dosud nekatalogizované položky majetku (vyjma nehmotných výsledků výzkumu a vývoje) je:
   a) fotografie reálně zobrazující dodávanou položku majetku ve formě elektronického souboru ve formátu JPG, rozlišení do 1024x768 bodů[3];
   b) hypertextový odkaz na webovou stránku nebo elektronický soubor, které obsahují technické údaje o výrobku. Elektronický soubor musí být ve formátu JPG, rozlišení do 1024x768 bodů, nebo ve formátu PDF, v rozměrech strany A4. V případě, že nelze poskytnout hypertextový odkaz nebo elektronický soubor, doložit správnost údajů nezbytných k provedení popisné identifikace jiným způsobem.
4. Zabezpečit doručení SPÚK OdKM v termínu do 30 dnů po ukončení řešení projektu.
5. Na vlastní náklady zabezpečit zpracování návrhu katalogizačních dat o výrobku popisnou metodou identifikace položek katalogizační agenturou[4] každé smlouvou definované položky zásobování vyrobené v ČR nebo zemích mimo NATO či Tier 2[5] a podléhající katalogizaci podle zásad NCS a JSK.
6. Zabezpečit doručení návrhu katalogizačních dat o výrobku (transakce LNC) nejpozději 60 dnů po ukončení řešení projektu.
7. Dodat bez prodlení písemně nebo elektronicky v průběhu realizace smlouvy informace o všech změnách, týkajících se předmětu smlouvy, které mají vliv na identifikaci katalogizovaných položek majetku, včetně změn u položek majetku nakupovaných příjemcem podpory od subdodavatelů.

Katalogizační doložka je naplněna dodáním úplných a bezchybných dat, které je potvrzeno po kontrole a zpracování dodaných dat vydáním kladného „Stanoviska Úř OSK SOJ k naplnění katalogizační doložky".

Přidělené identifikátory (KČM, NSN) a zpracovaná katalogizační data jsou dostupná na [redacted] ukončení procesu katalogizace majetku.

Kontaktní adresa:

Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti
ODDĚLENÍ KATALOGIZACE MAJETKU
nám. Svobody 471
160 01 PRAHA 6

TEL.:
E-MAIL:
INTERNET:

[redacted]

[redacted]

Elektronický podpis - 28.4.2022
Certifikát autora podpisu :
Jméno : Pavlína Čermáková
Vydal : ACAeID3.1 - Issuing Certificate
Platnost do : 7.7.2022 07:48:45-000 +02:00