Smlouva

o poskytnutí účelové podpory
na řešení projektu výzkumu, vývoje a inovací s názvem

„Výzkum nástrojů pro hodnocení kybernetické situace a podporu rozhodování CSIRT týmů při ochraně kritické infrastruktury“

VI20172020070

uzavřená mezi smluvními stranami

Česká republika – Ministerstvo vnitra

a

Masarykova univerzita

Č.j.MV-112904-4/OBVV-2016
Počet stran: 13
Přílohy: 2/15

Smluvní strany

Česká republika – Ministerstvo vnitra

se sídlem Nad Štolou 936/3, 170 34 Praha 7
IČ: 00007064
DIČ: CZ00007064
zastoupená ředitelem odboru bezpečnostního výzkumu a vzdělávání
JUDr. Petrem Novákem, Ph.D.
číslo bankovního účtu: [redacted]
adresa pro doručování: Ministerstvo vnitra, odbor bezpečnostního výzkumu a vzdělávání (gesční útvar MV ČR pro oblast bezpečnostního výzkumu), Nad Štolou 936/3, 170 34 Praha 7, tel.: [redacted], fax: [redacted], e-mail: [redacted]

(dále jen „**poskytovatel**")

a

Masarykova univerzita, Ústav výpočetní techniky

se sídlem Žerotínovo náměstí 617/9, 601 77 Brno
IČ: 00216224
DIČ: CZ00216224
statutární zástupce: doc. PhDr. Mikuláš Bek, Ph.D., rektor
uvedená v příloze č. 1 zákona č. 111/1998 Sb., o vysokých školách
číslo bankovního účtu: [redacted]
adresa pro doručování: sídlo příjemce

kontaktní osoba: [redacted] tel.: [redacted]; e-mail: [redacted]

(dále jen „**příjemce**")

uzavírají v rámci Programu bezpečnostního výzkumu České republiky v letech 2015 - 2020 (BV III/1 – VS), na základě § 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 č. 130/2002 Sb.") a v souladu se zákonem č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník") tuto

Smlouvu o poskytnutí účelové podpory
na řešení projektu výzkumu, vývoje a inovací
(dále jen „Smlouva")

Článek 1
Předmět Smlouvy

1) Předmětem této Smlouvy je závazek příjemce řešit projekt výzkumu, vývoje a inovací s názvem **„Výzkum nástrojů pro hodnocení kybernetické situace a podporu rozhodování CSIRT týmů při ochraně kritické infrastruktury"** a identifikačním kódem **„VI20172020070"** a závazek poskytovatele poskytnout příjemci na tento projekt účelovou podporu z veřejných prostředků (dále jen "podpora") v rozsahu a za podmínek stanovených Smlouvou.

2) Předmětem řešení projektu je průmyslový výzkum, zaměřený na výzkum nástrojů pro hodnocení bezpečnostní situace a podporu rozhodování bezpečnostního týmu (CSIRT) při ochraně kritických informačních struktur (KII). Nástroje budou sloužit členům CSIRT k rychlé orientaci v aktuální situaci s ohledem na probíhající kybernetické útoky, výskyt zranitelnosti a požadavků na důvěrnost, dostupnost a integritu KII. Nástroje budou sloužit k podpoře rozhodování bezpečnostního týmu výběrem optimální strategie použití reaktivních opatření.

3) Cíle projektu, předpokládané výsledky, rozpočet a harmonogram projektu, včetně dalších údajů jsou uvedeny ve schváleném projektu, který je přílohou č. 1 Smlouvy (dále jen „Projekt").

Článek 2
Administrátor Projektu

1) Administrátor Projektu je zaměstnanec gesčního útvaru pro oblast bezpečnostního výzkumu určený poskytovatelem, který je odpovědný za spolupráci a komunikaci s příjemcem ve všech záležitostech věcného plnění Projektu a finančního využití poskytnuté podpory.

2) Jméno a kontaktní údaje administrátora projektu budou příjemci sděleny při předání Smlouvy.

Článek 3
Manažer Projektu

Manažer Projektu určený příjemcem je odpovědný za řízení Projektu, včetně finančního řízení, za spolupráci a komunikaci s poskytovatelem.

Článek 4
Hlavní řešitel Projektu

Za odbornou úroveň Projektu dle § 9 odst. 1 písm. e) zákona č. 130/2002 Sb. je příjemci odpovědný XXXXXXXXXXXXXXXXX.

Článek 5
Doba řešení Projektu

1) Příjemce zahájí řešení Projektu dne 1.1.2017.

2) Příjemce je povinen ukončit řešení Projektu nejpozději ke dni 31.12.2020.

Článek 6
Uznané náklady, výše podpory a platební podmínky

1) Uznané náklady[1] na řešení Projektu se stanovují ve výši **12 853 000 Kč** (slovy: dvanáctmilionůosmsetpadesáttřitisíckorunčeských). Tato částka zahrnuje podporu ve výši **12 853 000 Kč** (slovy: dvanáctmilionůosmsetpadesáttřitisíckorunčeských), která je poskytovaná formou dotace z rozpočtové kapitoly Ministerstva vnitra.

[1] Uznané náklady jsou takové způsobilé náklady, které poskytovatel schválil a které jsou zdůvodněné.

2) Členění uznaných nákladů na jednotlivé položky a pro jednotlivé roky řešení Projektu je uvedeno v rozpočtu Projektu.

3) Nedojde-li v důsledku rozpočtového provizoria podle zákona č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů (dále jen „zákon o rozpočtových pravidlech") k regulaci čerpání rozpočtu, poskytovatel poskytne podporu příjemci v prvním roce řešení Projektu ve lhůtě do 60 kalendářních dnů ode dne nabytí účinnosti Smlouvy. V dalších letech řešení poskytovatel poskytne podporu do 60 kalendářních dnů od začátku kalendářního roku za podmínky, že jsou splněny závazky příjemce vyplývající ze Smlouvy, zejména, že příjemce předložil roční zprávu včetně vyúčtování poskytnutých finančních prostředků, a tato zpráva byla schválena poskytovatelem, a že jsou zařazeny údaje do informačního systému výzkumu, vývoje a inovací v souladu se zákonem č. 130/2002 Sb., Nařízením vlády č. 397/2009 Sb., o informačním systému výzkumu, experimentálního vývoje a inovací (dále jen „NV č. 397/2009 Sb.") a se zvláštním právním předpisem (zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů).

4) Pokud v průběhu řešení Projektu dojde ke snížení plánovaných finančních prostředků na výzkum a vývoj poskytovatele v rámci státního rozpočtu, je poskytovatel oprávněn jednostranně snížit podporu uvedenou v odst. 1 tohoto Článku a bude uzavřen písemný dodatek ke Smlouvě, v němž se vymezí související úpravy Projektu.

5) Podpora bude poskytována v souladu s rozpočtem bezhotovostním převodem z bankovního účtu poskytovatele na běžný korunový bankovní účet příjemce.

6) Příjemce má povinnost provést audit celého Projektu. Auditorskou zprávu předloží příjemce poskytovateli spolu se závěrečným vyúčtováním Projektu. Audit se týká všech nákladů Projektu. Do uznaných nákladů lze zahrnout pouze náklady na provedení auditu v závislosti na době realizace a účetní náročnosti Projektu až do výše 100 000 Kč.

Článek 7
Změny Rozpočtu

1) Podstatnou změnou rozpočtu, pro jejíž provedení je nutný předchozí souhlas poskytovatele se rozumí:

   a) zdůvodněná změna celkové výše rozpočtu příjemce,

   b) zdůvodněný přesun uvnitř rozpočtové skupiny mezi položkami přesahující 10 % celkových nákladů této skupiny v rámci rozpočtu příjemce v daném kalendářním roce,

   c) zdůvodněný přesun mezi rozpočtovými skupinami přesahující 10 % celkového rozpočtu příjemce v daném kalendářním roce.

2) Ostatní změny rozpočtu musí být se zdůvodněním oznámeny poskytovateli do 7 pracovních dnů od jejich provedení. Dojde-li k ostatní změně rozpočtu v měsíci prosinci, oznámí ji příjemce v roční zprávě za příslušný rok.

3) V případě, že součet objemu jednotlivých změn rozpočtu dle odst. 2 tohoto Článku v daném kalendářním roce dosáhne hranice stanovené v odst. 1 písm. b) nebo c) tohoto Článku, podléhá každá další změna rozpočtu předchozímu souhlasu poskytovatele.

4) Přesun finančních prostředků z rozpočtových skupin do rozpočtové skupiny osobní náklady a přesun finančních prostředků mezi jednotlivými položkami v rámci rozpočtové skupiny osobní náklady lze provést pouze s předchozím souhlasem poskytovatele.

5) Pokud příjemce neobdrží stanovisko poskytovatele do 15 kalendářních dnů ode dne odeslání informace o podstatné změně rozpočtu dle odst. 1 tohoto Článku nebo o změně dle odst. 3 a 4 tohoto Článku, považuje se změna rozpočtu za schválenou

poskytovatelem. Poskytovatel muze lhůtu prodloužit o 15 kalendářních dnů; je však povinen o prodloužení lhůty příjemce písemně informovat.

6) Žádosti příjemce o předchozí souhlas poskytovatele podle odst. 1 a 3 tohoto Článku i oznámení změny rozpočtu podle odst. 2 tohoto Článku předává příjemce prostřednictvím formuláře zveřejněného na webových stránkách Ministerstva vnitra včetně nové verze rozpočtu a komentáře popisujícího jeho změny.

7) Při postupu příjemce v rozporu s tímto Článkem bude postupováno dle Článku 20 odst. 3 Smlouvy.

Článek 8
Míra podpory

1) Mírou podpory se rozumí v procentech vyjádřený podíl výše podpory k uznaným nákladům příjemce v daném roce řešení Projektu.

2) Maximální povolená výše míry podpory činí 100 %.

Článek 9
Subdodávky

1) V rámci řešení Projektu nebudou realizovány subdodávky.

2) Pokud se v průběhu řešení Projektu vyskytne potřeba realizace subdodávky, postupuje příjemce podle zákona o veřejných zakázkách.

3) Subdodávky je příjemce povinen pořizovat za tržní ceny (tj. cena v místě a čase obvyklá). Toto je příjemce povinen poskytovateli doložit.

4) Subdodávky na výzkum nebo experimentální vývoj mohou být realizovány maximálně do výše 20 % celkových uznaných nákladů příjemce.

5) Nové subdodávky musí být předem odsouhlaseny poskytovatelem a upraveny písemným dodatkem ke Smlouvě.

6) Je-li subdodavatelem veřejně financovaná výzkumná organizace, mohou být předmětem subdodávek pouze výzkum nebo experimentální vývoj za těchto podmínek:

   a) výzkumná organizace poskytuje danou výzkumnou službu nebo provádí smluvní výzkum za tržní cenu nebo

   b) nelze-li určit tržní cenu, výzkumná organizace poskytne danou výzkumnou službu nebo provede smluvní výzkum za cenu, která zahrnuje plné náklady a přiměřený zisk.

7) Je-li příjemce výzkumnou organizací, může pořizovat subdodávky pouze od jiné výzkumné organizace.

8) Při pořízení subdodávek v rozporu s tímto Článkem bude postupováno dle Článku 20 Smlouvy.

Článek 10
Vedení účetnictví o uznaných nákladech Projektu

1) O vynaložených nákladech Projektu je příjemce povinen po celou dobu řešení Projektu vést v účetnictví oddělenou evidenci podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů v souladu s § 8 odst. 1 zákona č. 130/2002 Sb.

2) Nezpůsobilými náklady projektu jsou zejména:
   - zisk,

- daň z přidané hodnoty (u příjemců, kteří jsou plátci této daně a kteří uplatňují její odpočet nebo odpočet její poměrné části)[2],
- jiné daně (silniční daň, daň z nemovitosti, daň darovací, dědická, apod.),
- náklady na marketing, prodej a distribuci výrobků,
- úroky z dluhů,
- náklady na finanční pronájem a pronájem s následnou koupí (např. leasing, aj.),
- manka a škody,
- náklady na pohoštění, dary a reprezentaci,
- náklady na vydání periodických publikací, učebnic a skript,
- náklady/výdaje na pořízení budov a pozemků,
- opravy nebo údržba místností, stavby, rekonstrukce budov nebo místností, nábytek či zařízení, která nejsou pevnou součástí místností, a další náklady, které bezprostředně nesouvisejí s předmětem řešení projektu,
- správní poplatky,
- výdaje související s likvidací příjemce, nedobytné pohledávky,
- platby příspěvků do soukromých penzijních fondů,
- peněžitá pomoc v mateřství,
- ostatní sociální výdaje na zaměstnance, které nejsou zaměstnavatelé povinni odvádět dle zvláštních předpisů (např. dary k životním jubileím, příspěvky na rekreaci, příspěvky na penzijní připojištění, životní pojištění apod.),
- odstupné,
- nájemné, kdy příjemce je vlastníkem nemovitosti nebo ji užívá zdarma,
- výdaje na školení a vzdělávání personálu (pokud se nejedná o odborné akce přímo související s řešením projektu).

3) Do uznaných nákladů na pořízení hmotného a nehmotného majetku lze zahrnout pouze část ceny majetku, která odpovídá podílu užití majetku na řešení Projektu.

4) Příjemce účtuje doplňkové náklady související s Projektem **metodou kalkulace skutečných nákladů (FC - Full Costs)**.

5) Příjemce může finanční prostředky daného kalendářního roku, u kterých předpokládá jejich nevyčerpání, převést nejpozději do konce listopadu daného kalendářního roku na bankovní účet poskytovatele číslo (při převodu finančních prostředků příjemce uvede do Zprávy pro příjemce: VRATKA, kód projektu, název příjemce). Poskytovatel převede nevyčerpané finanční prostředky do nespotřebovaných nároků rozpočtu, aby mohly být použity ke stejnému účelu v dalším kalendářním roce. V případě, že v dalším kalendářním roce dojde ke snížení nároků z nespotřebovaných výdajů na základě rozhodnutí vlády dle § 47 odst. 6 písm. c) zákona o rozpočtových pravidlech, bude částka převedených finančních prostředků odpovídajícím způsobem snížena, případně nebude poskytnuta.

6) Je-li příjemce veřejnou výzkumnou institucí nebo veřejnou vysokou školou, může finanční prostředky, které nemohly být efektivně použity v roce, ve kterém byly poskytnuty, převést do fondu účelově určených prostředků, a to do výše 5% objemu těchto prostředků poskytnutých na Projekt v daném kalendářním roce. Takto převedené prostředky mohou být použity pouze k účelu, ke kterému byly poskytnuty[3]. Převod musí příjemce písemně oznámit poskytovateli a odůvodnit.

7) Jestliže příjemce převede finanční prostředky z Rozpočtu daného kalendářního roku do dalšího kalendářního roku ve svém účetnictví, s výjimkou odst. 6 tohoto Článku, je povinen tyto prostředky poskytovateli vrátit do 10. ledna následujícího roku převedením na bankovní účet poskytovatele číslo (při převodu finančních

[2] Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů
[3] § 18 odst. 10 a 11 zákona č. 111/1998 Sb., o vysokých školách; § 26 odst. 2 zákona č. 341/2005 Sb., o veřejných výzkumných institucích

prostředků příjemce uvede do Zprávy pro příjemce: VRATKA, kód projektu, název příjemce). Tyto prostředky budou poskytovatelem odvedeny do státního rozpočtu.

8) Pokud příjemce uplatňuje rozdílný hospodářský rok, provádí vyúčtování nákladů na Projekt a poskytnuté podpory k 31. 12. daného kalendářního roku a při uzávěrce hospodářského roku provede kontrolu tohoto vyúčtování a o výsledku písemně informuje poskytovatele.

Článek 11
Povinnosti příjemce

1) Příjemce je povinen postupovat při řešení Projektu v souladu s Projektem a dalšími podmínkami uvedenými ve Smlouvě.

2) Příjemce je povinen použít podporu v souladu s podmínkami, účelem a způsobem stanovenými Smlouvou. Použije-li příjemce podporu v rozporu s podmínkami stanovenými Smlouvou na jiný účel nebo jiným způsobem, závažným způsobem poruší povinnosti stanovené Smlouvou. V takovém případě bude postupováno dle Článku 20 odst. 4 Smlouvy.

3) Příjemce je povinen dodržovat podmínky uvedené v Projektu, na jejichž základě byla stanovena maximální povolená výše míry podpory. Porušení této povinnosti se pokládá za závažné porušení povinnosti a bude postupováno dle Článku 20 odst. 4 Smlouvy.

4) Příjemce je povinen předložit poskytovateli v každém příslušném roce řešení Projektu podklady pro účely vypořádání podpory se státním rozpočtem v souladu s § 14 odst. 10 a § 75 zákona o rozpočtových pravidlech a příslušnými předpisy pro zúčtování se státním rozpočtem platnými pro daný rok. O způsobu a termínech předložení podkladů bude příjemce ze strany poskytovatele každoročně písemně informován.

5) Příjemce je povinen písemně informovat poskytovatele o veškerých podstatných skutečnostech, které by mohly mít vliv na průběh a výsledek řešení Projektu a které nastaly v době ode dne nabytí platnosti a účinnosti Smlouvy, a to ve lhůtě do 15 kalendářních dnů ode dne, kdy se o takové skutečnosti dozvěděl.

6) Podstatnou změnou, pro jejíž provedení je nutný předchozí souhlas poskytovatele je změna harmonogramu projektu, změna výsledků projektu, změna data ukončení řešení projektu, změna manažera Projektu, změna hlavního řešitele Projektu a změna řešitelů Projektu. Pokud příjemce neobdrží stanovisko poskytovatele do 15 kalendářních dnů ode dne odeslání informace o podstatné změně, považuje se podstatná změna za schválenou poskytovatelem. Poskytovatel může lhůtu prodloužit o 15 kalendářních dnů; je však povinen o prodloužení lhůty příjemce písemně informovat. Formulář pro informování poskytovatele příjemcem dle tohoto ustanovení je zveřejněn na webových stránkách Ministerstva vnitra. Při postupu příjemce v rozporu s tímto ustanovením, bude postupováno dle ustanovení Článku 20 odst. 3 Smlouvy.

7) O ostatních změnách informuje příjemce poskytovatele průběžně, nejpozději v roční zprávě dle Článku 12 odst. 2 Smlouvy.

8) Příjemce je povinen každou zahraniční pracovní cestu, jejíž náklady přesáhnou 60 000 Kč, předložit s předstihem nejméně 30 kalendářních dní před zahájením zahraniční pracovní cesty se zdůvodněním poskytovateli ke schválení. Nejpozději do 30 kalendářních dní po ukončení cesty je příjemce povinen předložit poskytovateli podrobnou zprávu o jejím průběhu a výsledcích ve vztahu k řešení Projektu.

9) Veškerá oznámení dle tohoto Článku předává příjemce formou a ve lhůtách, které jsou uvedeny ve Smlouvě.

10) Příjemce je povinen poskytnout i další údaje požadované poskytovatelem pro věcné a finanční řízení Projektu, a to v termínech stanovených poskytovatelem.

Článek 12
Zprávy

1) Příjemce předkládá poskytovateli ke schválení v průběhu řešení Projektu zprávy o průběhu řešení Projektu (roční zprávy, mimořádné zprávy). Po ukončení řešení Projektu příjemce předloží poskytovateli závěrečnou zprávu.

2) Roční zprávu je příjemce povinen předložit poskytovateli za každý rok řešení Projektu vždy ve lhůtě do 20. ledna následujícího kalendářního roku, nestanoví-li poskytovatel písemně jinak. Roční zpráva obsahuje zejména informace o postupu řešení Projektu, o dosažených výsledcích a způsobu jejich využití v uplynulém roce. V roční zprávě zároveň příjemce upřesní postup řešení Projektu na další rok a předloží aktuální verzi harmonogramu. Samostatnou částí roční zprávy je vyúčtování nákladů na Projekt a poskytnuté podpory za uplynulý rok ve struktuře Rozpočtu a aktuální verze rozpočtu.

3) Mimořádnou zprávu předkládá příjemce poskytovateli v průběhu řešení Projektu na vyžádání poskytovatele, který zároveň stanoví předmět zprávy a termín jejího předložení.

4) Závěrečnou zprávu z řešení Projektu předloží příjemce do 30 kalendářních dnů ode dne ukončení řešení Projektu uvedeného v Článku 5 Smlouvy. Závěrečná zpráva z řešení Projektu zahrnuje zejména informaci o dosažených cílech, výsledcích, způsobu jejich využití a výstupech Projektu. Součástí závěrečné zprávy je vyúčtování nákladů na Projekt a poskytnuté podpory za celé období řešení Projektu ve struktuře Rozpočtu.

5) Příjemce je povinen předkládat poskytovateli zprávu o využití výsledků Projektu v souladu s Popisem výsledků projektu a plánem jejich využití, který je přílohou č. 2 Smlouvy, a to každoročně po dobu 5 let ode dne ukončení Smlouvy, vždy ve lhůtě do 20. ledna následujícího kalendářního roku.

6) U Projektů obsahujících utajované informace budou zprávy uvedené v tomto Článku zpracovávány v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon č. 412/2005 Sb.").

7) Poskytovatel stanoví rozsah, strukturu a formu zpráv uvedených v tomto Článku.

8) Poskytovatel schvaluje roční a mimořádné zprávy nejpozději do 30 kalendářních dnů ode dne jejich doručení nebo v této lhůtě uplatní písemné připomínky a stanoví lhůtu pro jejich vypořádání příjemcem.

9) Pokud příjemce nepředloží zprávy uvedené v odst. 1 až 4 tohoto Článku, bude postupováno dle Článku 20 odst. 3 Smlouvy.

Článek 13
Kontroly

1) Poskytovatel je oprávněn ve smyslu § 13 zákona č. 130/2002 Sb. provádět u příjemce kontrolu plnění cílů Projektu, včetně kontroly čerpání a využívání podpory a účelnosti vynaložených prostředků podle této Smlouvy.

2) Poskytovatel je oprávněn provádět finanční kontrolu v souladu se zákonem č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů a provádět kontrolu podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád).

3) Příjemce je povinen umožnit poskytovateli provedení všech kontrol uvedených v odstavci 1 a 2 tohoto Článku a poskytnout mu při nich potřebnou součinnost, zejména poskytnout na pracovištích příjemce volný přístup k osobám podílejícím se na řešení Projektu, ke všem dokumentům, počítačovým záznamům a zařízením, která přísluší k řešení Projektu.

4) Příjemce je povinen předložit na žádost poskytovatele pro potřeby kontroly Projektu originály veškerých účetních dokladů vztahujících se k Projektu.

5) Příjemce je povinen předkládat poskytovateli na vyžádání přehledy jakýchkoliv účetních záznamů vztahujících se k Projektu.

6) Osoby provádějící kontrolu jsou povinny předložit příjemci písemné pověření ředitele věcně příslušného odboru poskytovatele k provedení kontroly.

7) Kontrolu je poskytovatel oprávněn provést kdykoliv v době řešení Projektu a následně ve lhůtě do 5 let ode dne ukončení Smlouvy. Příjemce je povinen po celou tuto dobu uchovávat veškeré doklady týkající se Projektu.

Článek 14
Nákup a vlastnictví majetku pořízeného pro řešení Projektu

1) V rámci řešení Projektu příjemce nebude pořizovat hmotný a nehmotný majetek.

2) Pokud se v průběhu řešení Projektu vyskytne potřeba pořídit hmotný a nehmotný majetek, postupuje se podle zákona o veřejných zakázkách.

3) Hmotný a nehmotný majetek je příjemce povinen pořizovat za tržní ceny (tj. cena v místě a čase obvyklá). Toto je příjemce povinen poskytovateli doložit.

4) Vlastníkem majetku, pořízeného z poskytnuté podpory je ve smyslu ustanovení § 15 odst. 1 zákona č. 130/2002 Sb. příjemce.

5) Při pořízení majetku v rozporu s tímto Článkem bude postupováno dle Článku 20 Smlouvy.

Článek 15
Práva k výsledkům Projektu a jejich využití

1) Práva k výsledkům Projektu patří příjemci.

2) Při využití výsledků Projektu je příjemce povinen postupovat v souladu s ustanovením § 16 odst. 4 zákona č. 130/2002 Sb., Popisem výsledků projektu a plánem jejich využití.

Článek 16
Poskytování informací

1) Příjemce je povinen předávat poskytovateli veškeré informace o Projektu pro účely jejich předání do informačního systému výzkumu, experimentálního vývoje a inovací ve formě a termínech stanovených poskytovatelem v souladu se zákonem č. 130/2002 Sb. a NV č. 397/2009 Sb., a další informace stanovené poskytovatelem.

2) Při jakémkoliv předávání nebo zveřejňování informací týkajících se Projektu a výsledků Projektu, včetně konferencí, je příjemce povinen zveřejnit informaci o poskytnuté podpoře poskytovatelem na základě Smlouvy a o příslušnosti k programu výzkumu a vývoje poskytovatele.

3) Pokud je předmět řešení Projektu utajovanou informací podle zákona č. 412/2005 Sb., je příjemce povinen uvést stupeň důvěrnosti těchto údajů podle zákona č. 412/2005 Sb., a poskytnout poskytovateli konkrétní informace o Projektu a jeho výsledcích postupem podle zákona č. 130/2002 Sb.

4) Příjemce je povinen při změně Smlouvy předat poskytovateli informace o změně údajů zveřejňovaných v informačním systému výzkumu, experimentálního vývoje a inovací, pokud k takovéto změně v důsledku změny Smlouvy dojde.

Článek 17
Povinnost mlčenlivosti

1) Poskytovatel a příjemce jsou povinni zajistit mlčenlivost o všech informacích, které jim jako důvěrné byly poskytnuty a jejichž předání dalším subjektům by mohlo poškodit práva toho, kdo je poskytl.

2) V případě, že jsou poskytovatel a příjemce na základě Smlouvy oprávněni poskytovat informace třetím stranám, jsou povinni zajistit, aby tyto třetí strany zachovávaly mlčenlivost o těchto informacích, které jim byly poskytnuty jako důvěrné, a používaly je jen k účelům, k nimž jim byly předány.

3) Poskytovatel a příjemce jsou zproštěni povinnosti zachovávat mlčenlivost v případě:

   a) že se obsah informací, které jim byly poskytnuty jako důvěrné, stane veřejně přístupným, a to na základě jiných činností prováděných mimo rámec Smlouvy nebo na základě opatření, která nesouvisí s řešením Projektu;

   b) že byl požadavek zachovávat mlčenlivost odvolán těmi, v jejichž prospěch byla tato povinnost stanovena.

Článek 18
Odpovědnost za škodu

1) Odpovědnost za škodu se řídí ustanoveními občanského zákoníku.

2) Poskytovatel neodpovídá za jednání nebo za nečinnost příjemce. Poskytovatel neodpovídá za nedostatky výrobků vytvořených nebo služeb poskytnutých na základě výsledků Projektu.

3) Příjemce se zavazuje, že odškodní třetí strany v případě uplatnění požadavku na náhradu škody, která vznikla jednáním nebo nečinností příjemce nebo která souvisí s nedostatky výrobků vytvořených nebo služeb poskytnutých na základě výsledků Projektu, pokud neprokáže, že za tyto neodpovídá.

4) Prokáže-li třetí strana své nároky spojené s prováděním Smlouvy vůči poskytovateli, je příjemce povinen poskytovateli poskytnout pomoc.

Článek 19
Odstoupení od Smlouvy

1) Poskytovatel je oprávněn od Smlouvy odstoupit v případě, že:

   a) příjemce uvedl neúplné, nesprávné nebo nepravdivé údaje a skutečnosti ve veřejné soutěži nebo při uzavření Smlouvy;

   b) příjemce nesplnil povinnosti nebo jiné podmínky stanovené Smlouvou ani poté, co jej poskytovatel k tomu písemně vyzval a stanovil mu náhradní dobu k jejich splnění; náhradní doba k plnění nesmí být kratší než 30 kalendářních dnů;

   c) příjemce vstoupil do likvidace nebo na něho byla vyhlášena nucená správa, vůči majetku příjemce probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh nebyl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo nebyl konkurs zrušen proto, že majetek byl zcela nepostačující, byla povolena reorganizace nebo byl nařízen výkon rozhodnutí prodejem podniku, pokud by tato skutečnost mohla dle názoru poskytovatele ovlivnit řešení Projektu nebo zájmy poskytovatele;

   d) dojde ke vzniku závažných ekonomických nebo technických důvodů, které podstatně ovlivní řešení Projektu, nebo se výrazně sníží možnost využití poznatků Projektu;

   e) z důvodu podstatného porušení Smlouvy podle § 2002 odst. 1 občanského zákoníku.

2) Odstoupení od Smlouvy musí být odůvodněno a nabývá účinnosti dnem jeho doručení příjemci.

Článek 20
Vrácení podpory a sankce

1) V případě odstoupení od Smlouvy podle ustanovení Článku 19 odst. 1 písm. a), b) a e) Smlouvy je příjemce povinen vrátit poskytnutou podporu poskytovateli v plné výši. K vrácené podpoře je příjemce povinen zaplatit smluvní pokutu ve výši 0,1 % z částky podpory uvedené v Projektu pro rok, v němž vznikl důvod k odstoupení od Smlouvy, a to za každý den za dobu ode dne připsání poskytnuté podpory, která má být vrácena, na bankovní účet příjemce do dne jejího připsání na účet poskytovatele.

2) V případě odstoupení od Smlouvy podle ustanovení Článku 19 odst. 1 písm. c) a d) Smlouvy a v případě uzavření dohody o ukončení Smlouvy je příjemce povinen vrátit poskytnutou podporu v poměrné výši, stanovené poskytovatelem, a to ve lhůtě do 30 kalendářních dnů ode dne doručení sdělení o odstoupení od Smlouvy nebo ode dne nabytí účinnosti dohody o ukončení Smlouvy. Z poskytnuté podpory mohou být uhrazeny jen uznané náklady Projektu použité příjemcem na poskytovatelem schválené výstupy z Projektu, kterých bylo dosaženo do okamžiku odstoupení od Smlouvy, případně ukončení Smlouvy dohodou.

3) V případě, že příjemce neinformuje poskytovatele dle Článku 7 odst. 1 až 3, Článku 11 odst. 6, Článku 12 odst. 1 až 4 této Smlouvy, poskytovatel uloží příjemci smluvní pokutu ve výši 2 % z částky podpory uvedené v Projektu pro rok, v němž vznikl důvod k uložení smluvní pokuty. Podpora pro následující kalendářní rok bude příjemci poskytnuta ve výši, snížené o uplatněnou smluvní pokutu.

4) V případě, že příjemce použije poskytnutou podporu nebo část poskytnuté podpory v rozporu s podmínkami, účelem nebo způsobem stanovenými touto Smlouvou, je poskytovatel oprávněn požadovat od příjemce vrácení takto použitých prostředků. Příjemce je povinen tyto prostředky převést na účet poskytovatele, a to ve lhůtě do 30 kalendářních dnů ode dne, kdy byl tento požadavek poskytovatele písemně doručen příjemci.

5) V případě, že příjemce nevyužije výsledky Projektu nebo neumožní jejich využití dle § 16 odst. 4 zákona č. 130/2002 Sb., vrátí poskytovateli poskytnutou podporu v plné výši.

6) V případě, že u příjemce byly po ukončení Smlouvy zjištěny na základě provedené kontroly závažné finanční nesrovnalosti nebo podvod, může poskytovatel od příjemce písemně požadovat vrácení poskytnuté podpory v celé výši. K vrácené podpoře je příjemce povinen zaplatit smluvní pokutu ve výši 0,1 % z poskytnuté podpory za každý den, a to za dobu ode dne připsání poskytnuté podpory, která má být vrácena, na bankovní účet příjemce do dne jejího připsání na účet poskytovatele.

7) Poskytnutá podpora nebo její poměrná část se vrací a smluvní pokuta se platí připsáním na bankovní účet poskytovatele, který bude příjemci poskytovatelem sdělen.

8) Neoprávněné použití nebo zadržení podpory se posuzuje jako porušení rozpočtové kázně podle zákona o rozpočtových pravidlech.

9) Poskytovatel je oprávněn přerušit nebo zastavit poskytování podpory příjemci, pokud jsou naplněny skutkové podstaty, pro které může být Smlouva ukončena v souladu s ustanovením Článku 19 odst. 1 Smlouvy. Ustanovením tohoto odstavce nejsou dotčena práva poskytovatele stanovená Smlouvou. Příjemci nenáleží náhrada škody, která mu vznikne v důsledku přerušení nebo zastavení poskytování podpory.

10) Tímto Článkem není dotčen nárok poskytovatele na náhradu škody, která mu vznikne v důsledku neplnění Smlouvy příjemcem.

Článek 21
Ukončení řešení Projektu a ukončení Smlouvy

1) Příjemce je povinen řešení Projektu ukončit nejpozději ke dni uvedenému v Článku 5 Smlouvy. Řešení Projektu se považuje za ukončené rovněž v případě předčasného zastavení řešení Projektu v souvislosti s ukončením Smlouvy v souladu s ustanovením tohoto Článku odst. 4 písm. b) a c) Smlouvy.
2) Po ukončení řešení Projektu poskytovatel provede závěrečné hodnocení Projektu, zejména zhodnocení plnění cílů Projektu, včetně kontroly čerpání a využívání podpory, účelnosti vynaložených prostředků Projektu podle Smlouvy a dále provede závěrečné zhodnocení dosažených výsledků Projektu a jejich vztah k cílům Projektu.
3) Smlouva je splněna dnem schválení závěrečné zprávy poskytovatelem a úspěšným závěrečným hodnocením Projektu poskytovatelem v souladu s § 13 odst. 4 zákona č. 130/2002 Sb.
4) Smlouva je ukončena:
   a) dnem ukončení Smlouvy stanoveným ve Smlouvě v Článku 25 odst. 2,
   b) dnem doručení písemného odstoupení od Smlouvy poskytovatelem,
   c) dnem nabytí účinnosti dohody smluvních stran o ukončení Smlouvy.
5) Po ukončení Smlouvy je poskytovatel oprávněn podle § 9 odst. 1 písm. k) zákona č. 130/2002 Sb. provádět u příjemce kontrolu využití výsledků Projektu v souladu s § 16 zákona č. 130/2002 Sb., Popisem výsledků projektu a plánem jejich využití, a to ve lhůtě do 5 let ode dne ukončení Smlouvy.

Článek 22
Doručování písemností

1) Písemnosti dle Smlouvy se doručují na adresu poskytovatele nebo příjemce uvedenou v této Smlouvě. V případě doručování prostřednictvím provozovatele poštovní služby je náhradní doručení uložením zásilky možné. V takovém případě se považuje písemnost za doručenou 10. kalendářní den ode dne oznámení o uložení zásilky na poště.
2) Písemnosti v elektronické formě lze doručovat do datové schránky poskytovatele nebo příjemce podle zvláštního zákona[4], s výjimkou ustanovení Článku 12 odst. 6 Smlouvy. Písemnost se považuje za doručenou nejpozději 10. kalendářní den ode dne, kdy byl dokument dodán do datové schránky.

Článek 23
Spory smluvních stran

Spory smluvních stran vznikající ze Smlouvy nebo v souvislosti s ní, budou řešeny příslušným soudem.

Článek 24
Závěrečná ustanovení

1) Smlouva, včetně příloh, může být doplňována, upravována a měněna pouze písemnými, po sobě číslovanými dodatky ke Smlouvě, podepsanými smluvními stranami.

[4] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

2) Nestanoví-li Smlouva jinak, návrh posledního dodatku ke Smlouvě lze doručit druhé smluvní straně nejpozději 60 kalendářních dnů přede dnem ukončení řešení Projektu uvedeným v Článku 5 Smlouvy.

3) Smlouva se řídí právním řádem České republiky.

4) Vztahy neupravené Smlouvou se řídí především zákonem č. 130/2002 Sb. a občanským zákoníkem.

5) Základní ustanovení Smlouvy (Články 1 až 25 Smlouvy) mají v případě rozporu přednost před ustanoveními Projektu.

6) Nedílnou součástí Smlouvy jsou:

   a) Příloha č. 1 - Projekt,

   b) Příloha č. 2 - Popis výsledků projektu a plán jejich využití.

7) Smlouva se vyhotovuje ve dvou stejnopisech, z nichž poskytovatel i příjemce obdrží po jejich podpisu jedno vyhotovení.

8) Smluvní strany prohlašují a podpisem Smlouvy stvrzují, že jimi uvedené údaje, na jejichž základě je uzavřena Smlouva a poskytnuta podpora poskytovatelem, jsou správné, úplné a pravdivé.

9) Smluvní strany prohlašují, že si tuto Smlouvu přečetly, s jejím obsahem souhlasí a že byla sepsána na základě jejich pravé a svobodné vůle, a na důkaz toho připojují své podpisy.

Článek 25
Platnost a účinnost Smlouvy

1) Smlouva se uzavírá na dobu určitou a nabývá platnosti dnem podpisu smluvních stran a účinnosti dnem 1.1.2017.

2) Smlouva je ukončena 29.6.2021.

3) Ukončení Smlouvy před datem uvedeným v odst. 2 tohoto Článku je upraveno v ustanovení Článku 21 odst. 4 písm. b) a c) Smlouvy.

Za poskytovatele: [redacted]

JUDr. Petr Novák, Ph.D.

V Praze dne: 3. 10. 2016

Za příjemce: [redacted]

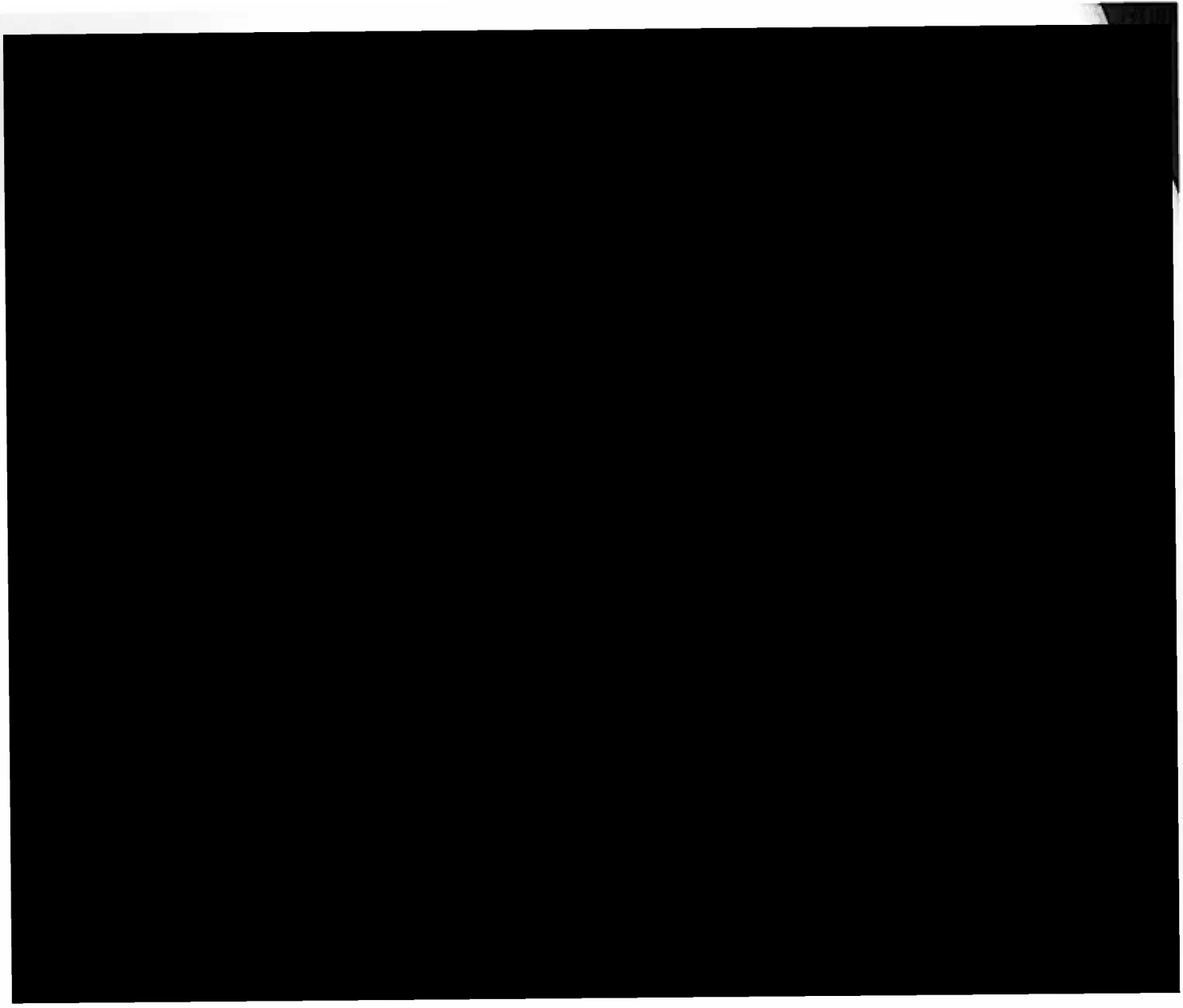
doc. PhDr. Mikuláš Bek, Ph.D.

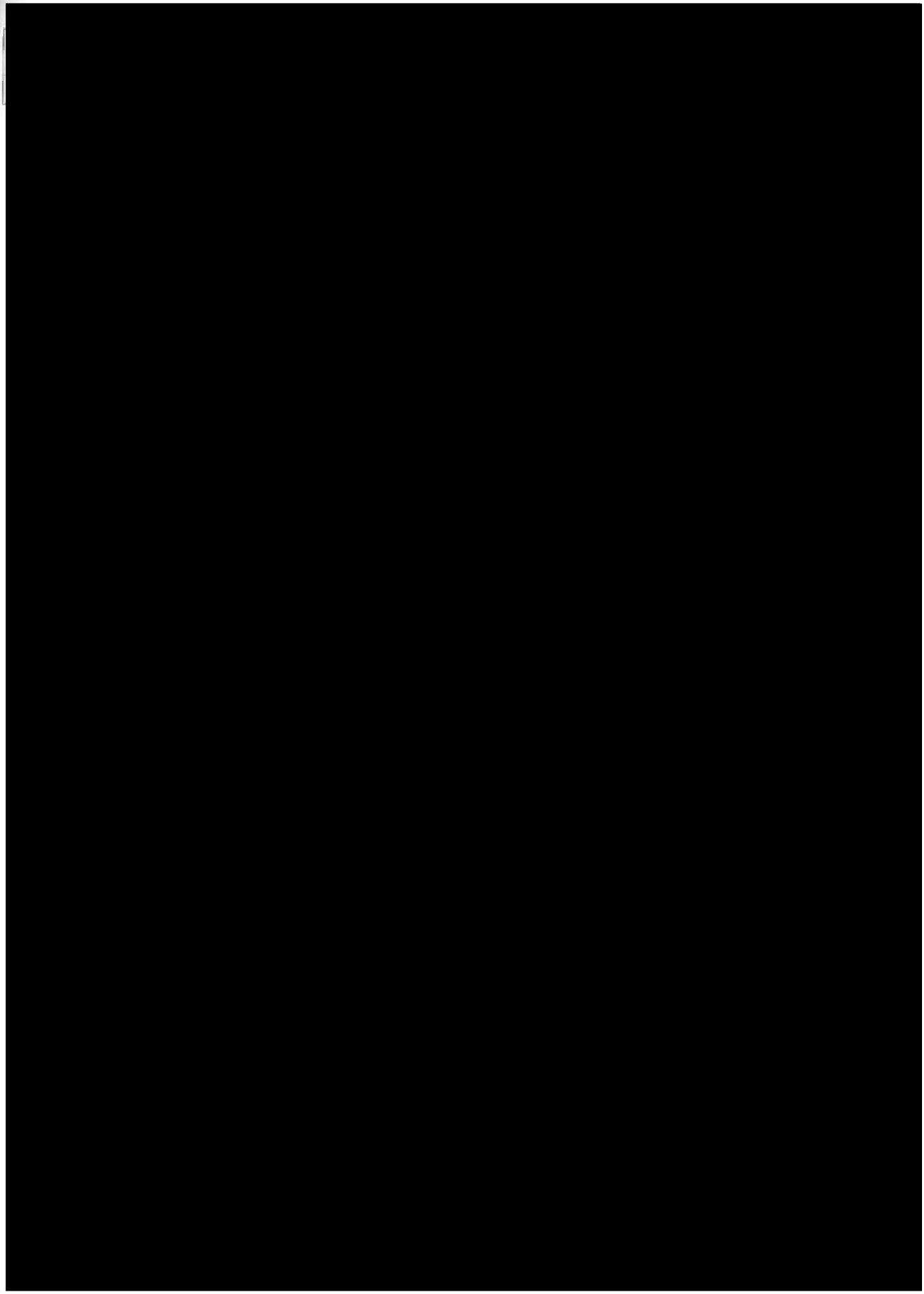
V Brně dne: 10. 10. 2016

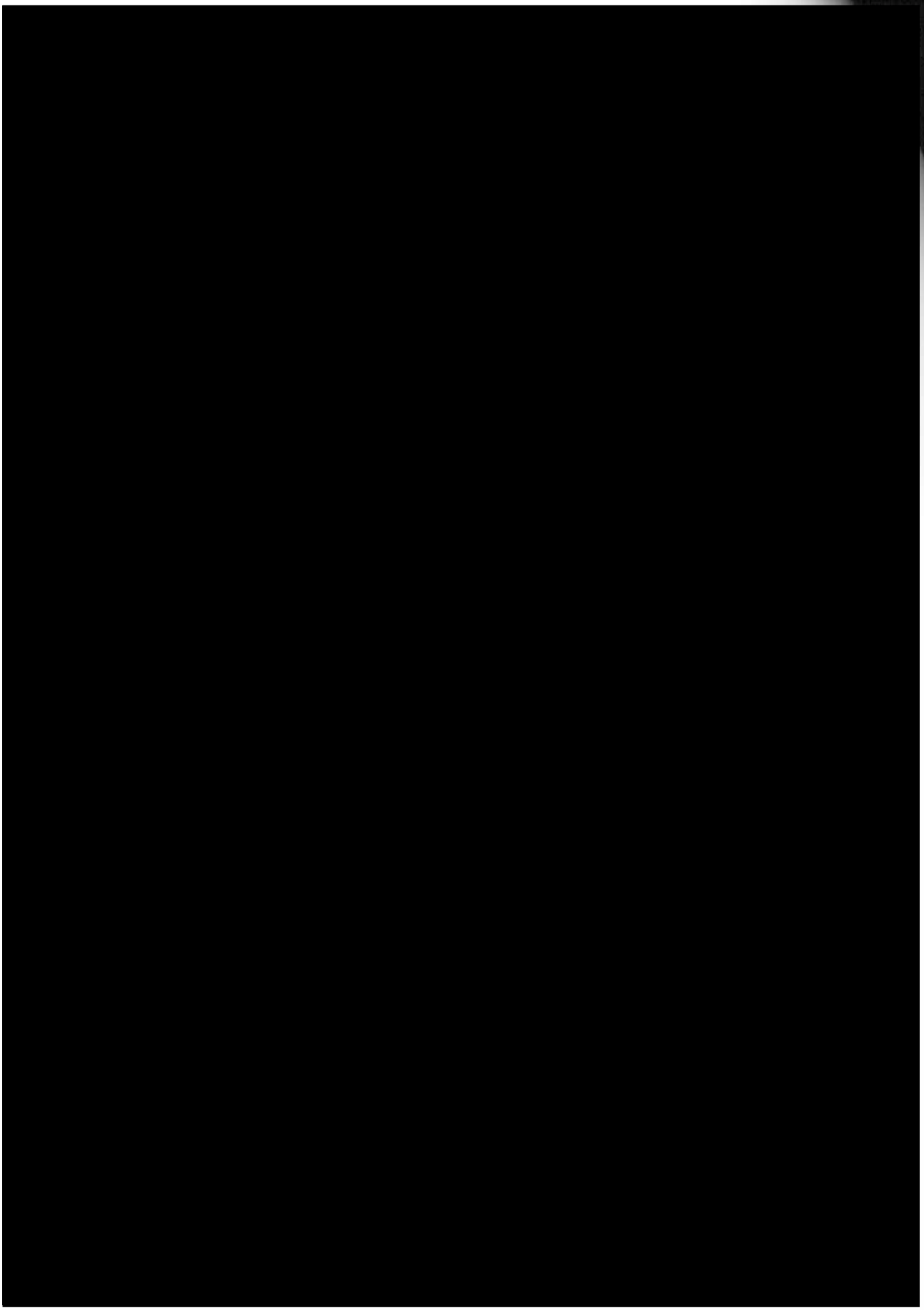
[redacted]

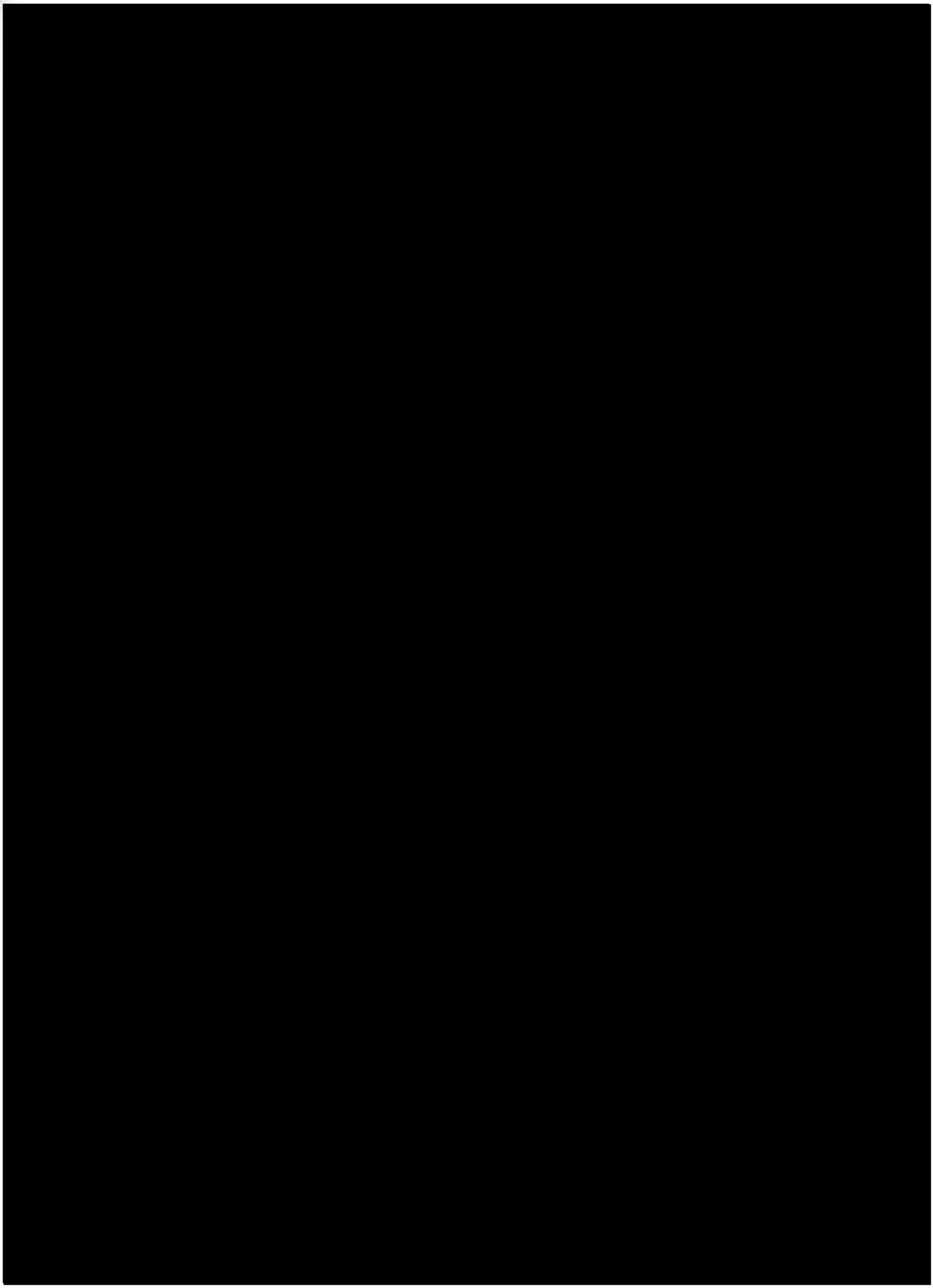
Příloha č. 1
k č. j. MV-112904-4/OBV-2016

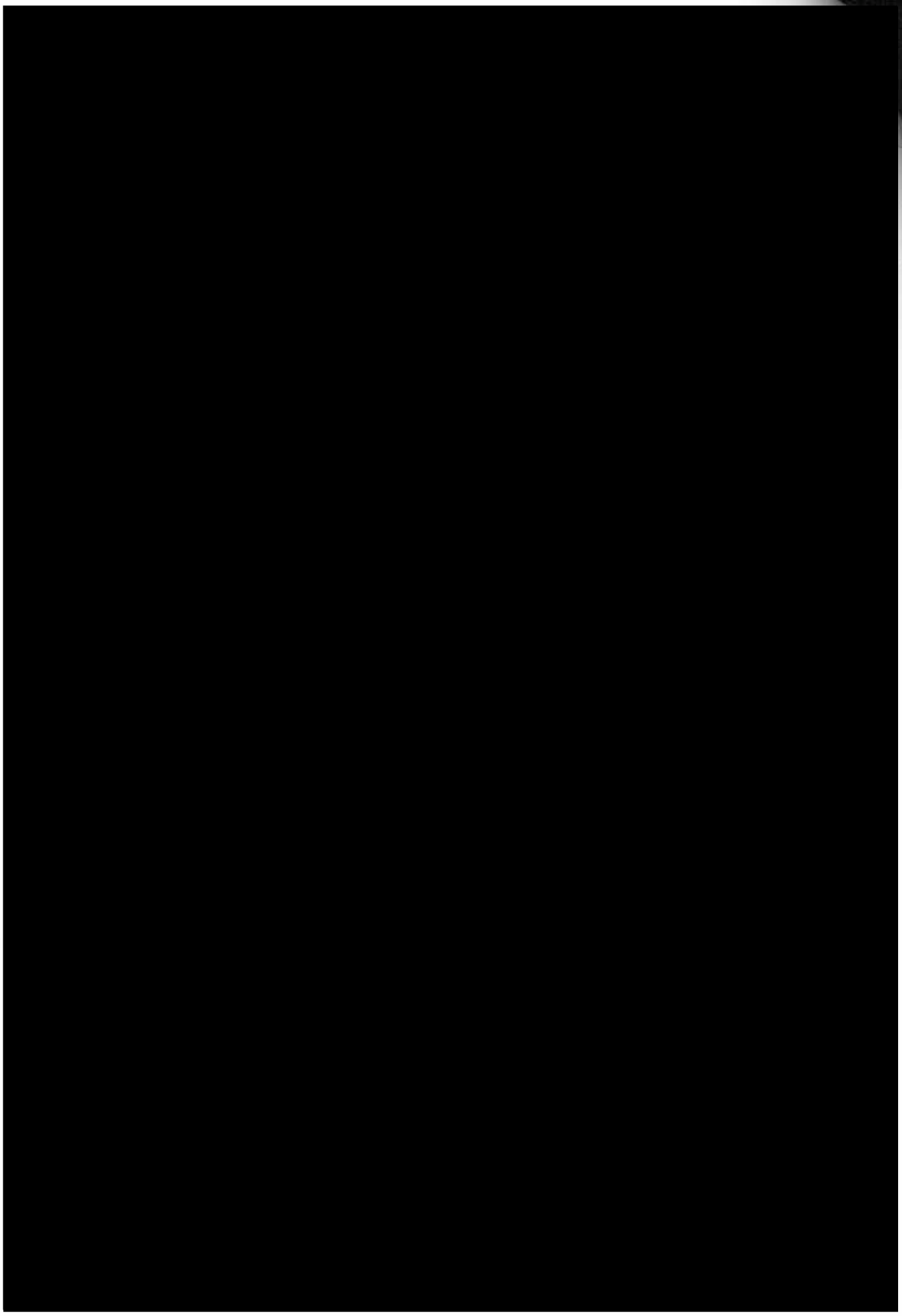
[redacted]

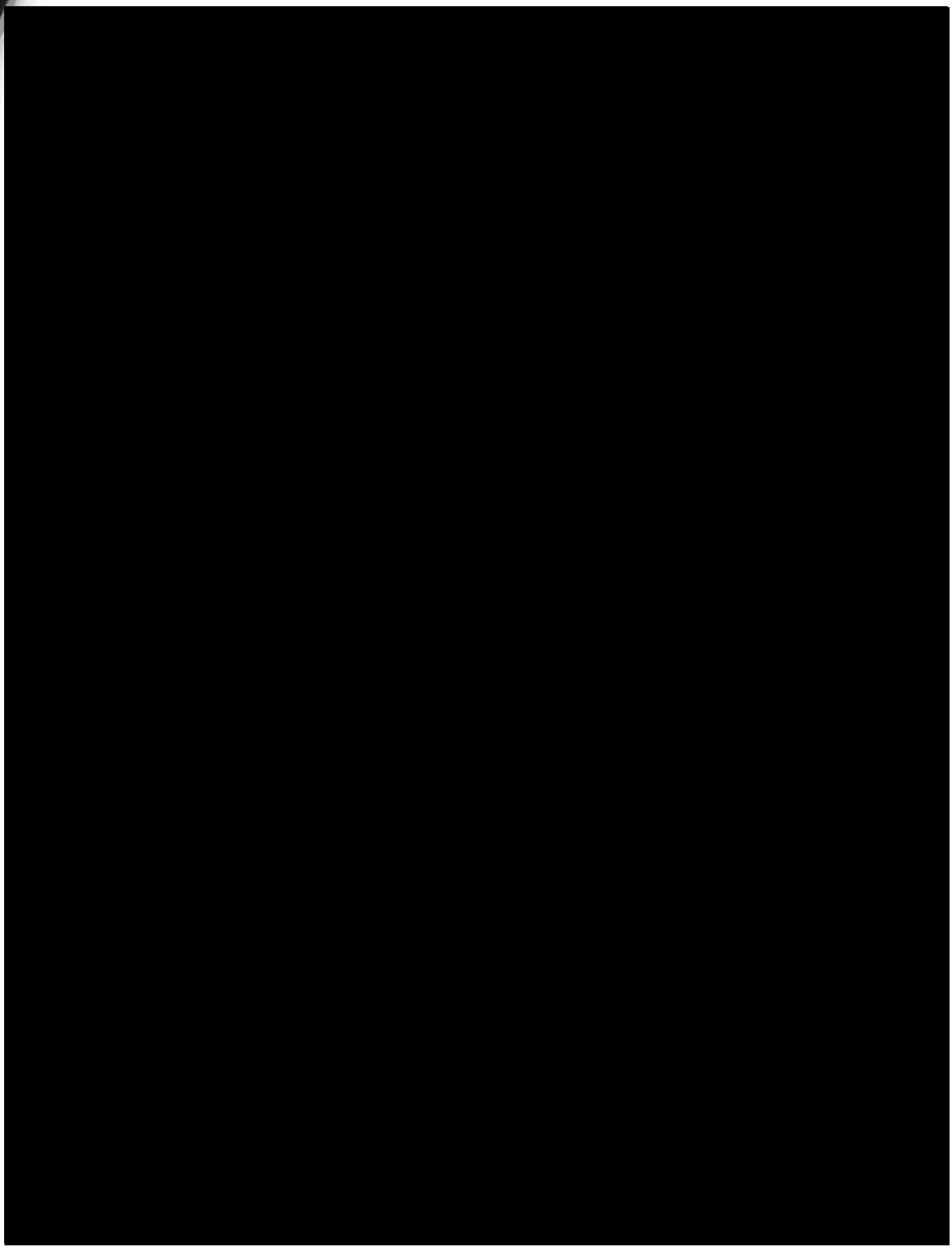


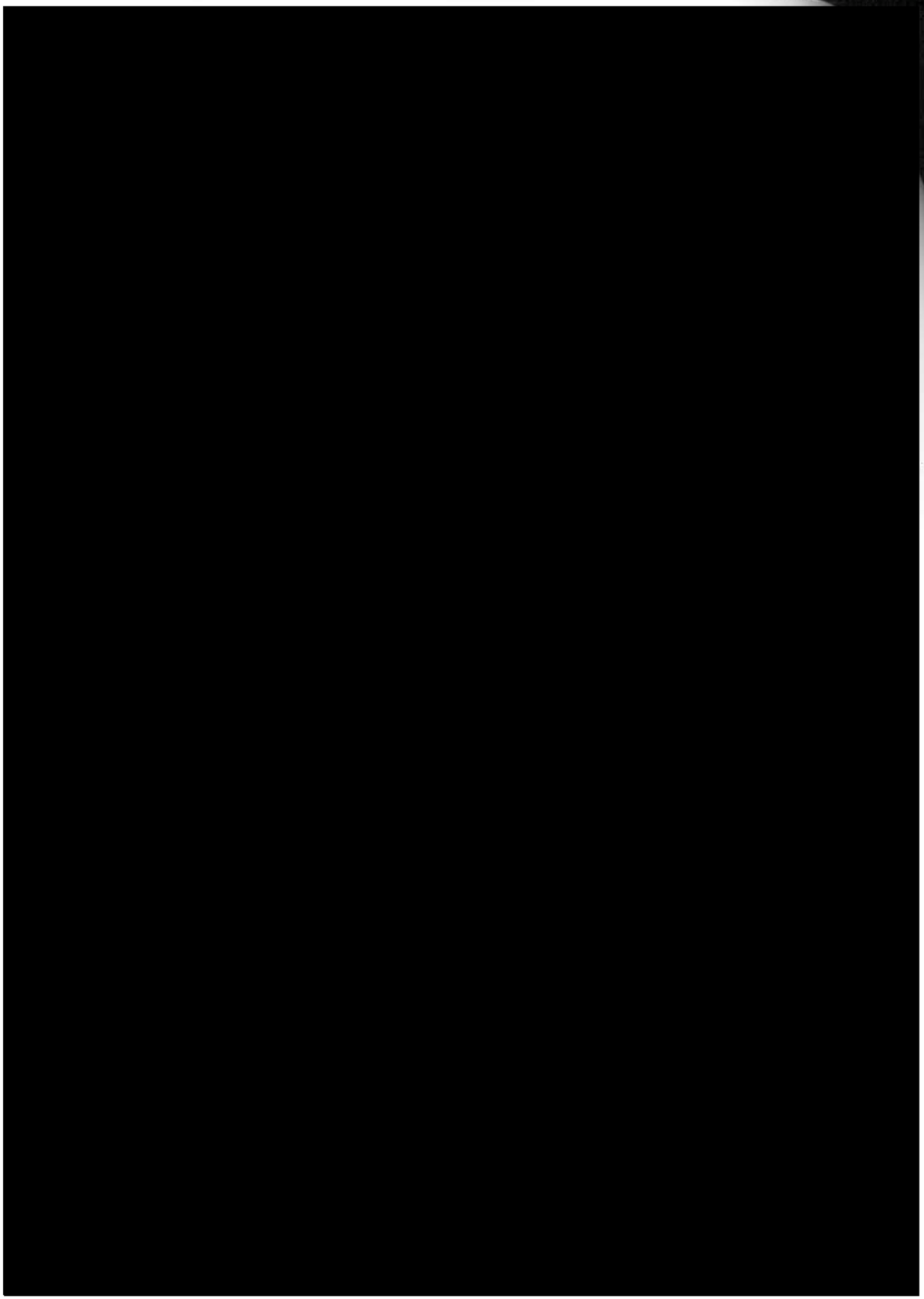


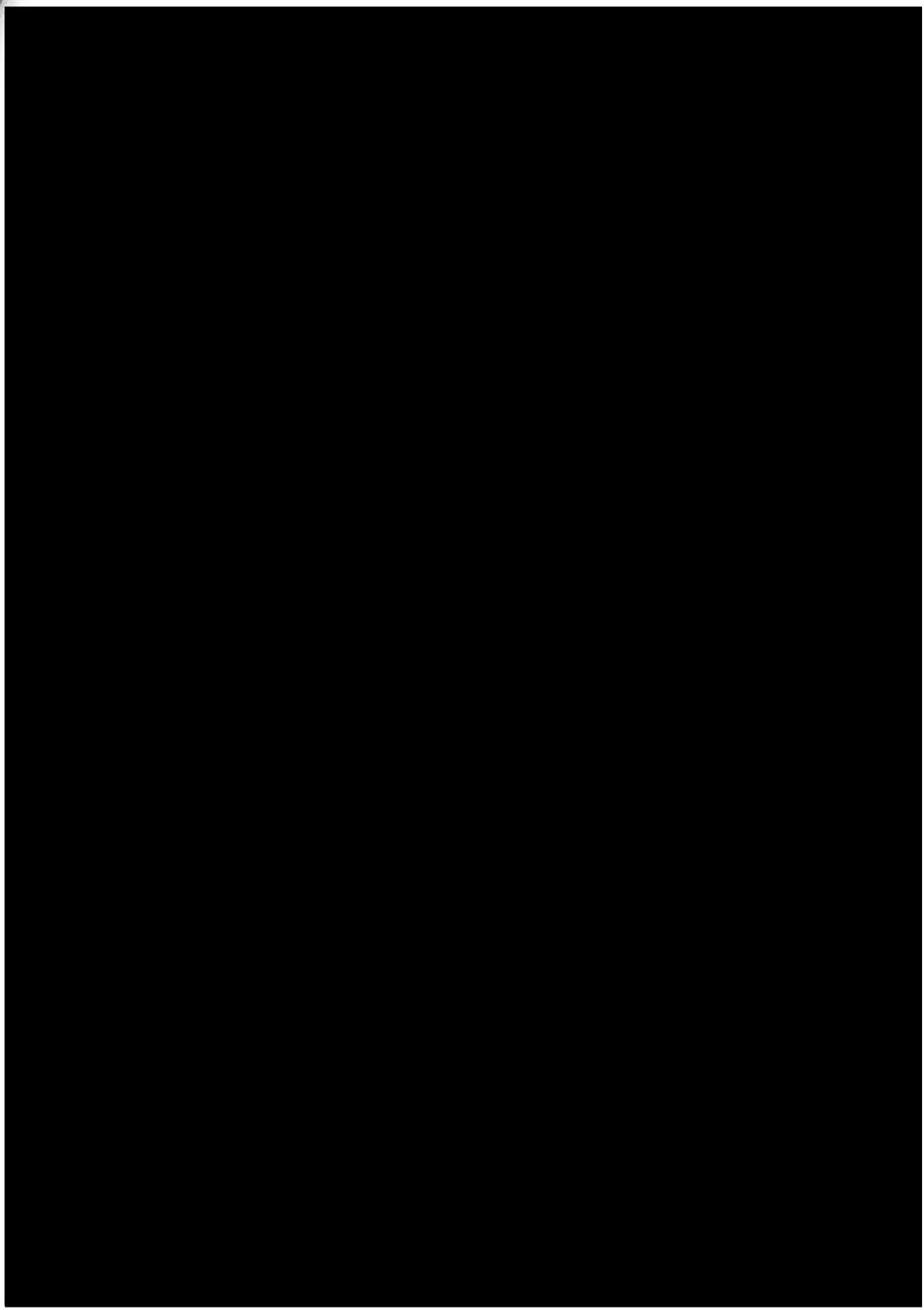


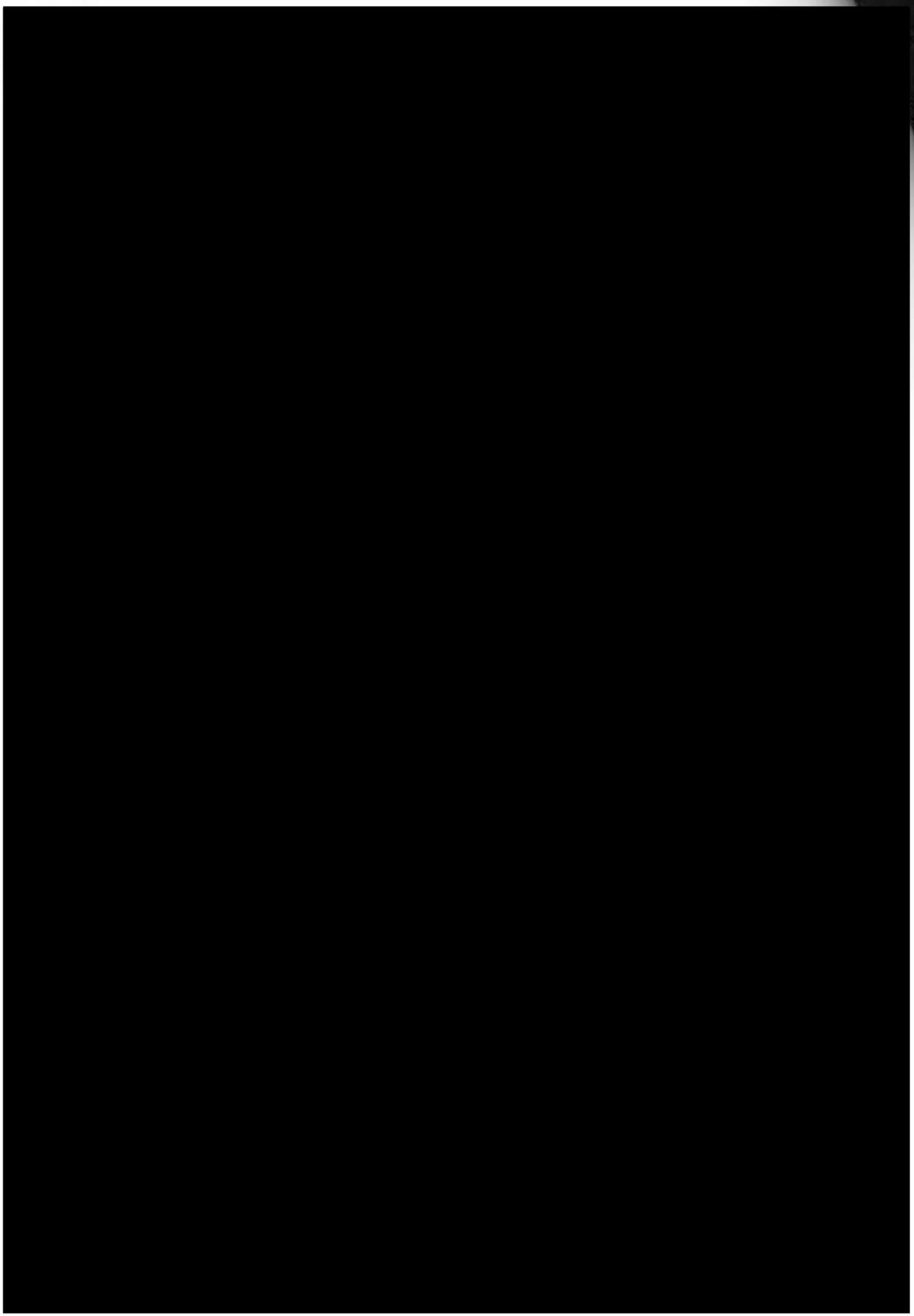


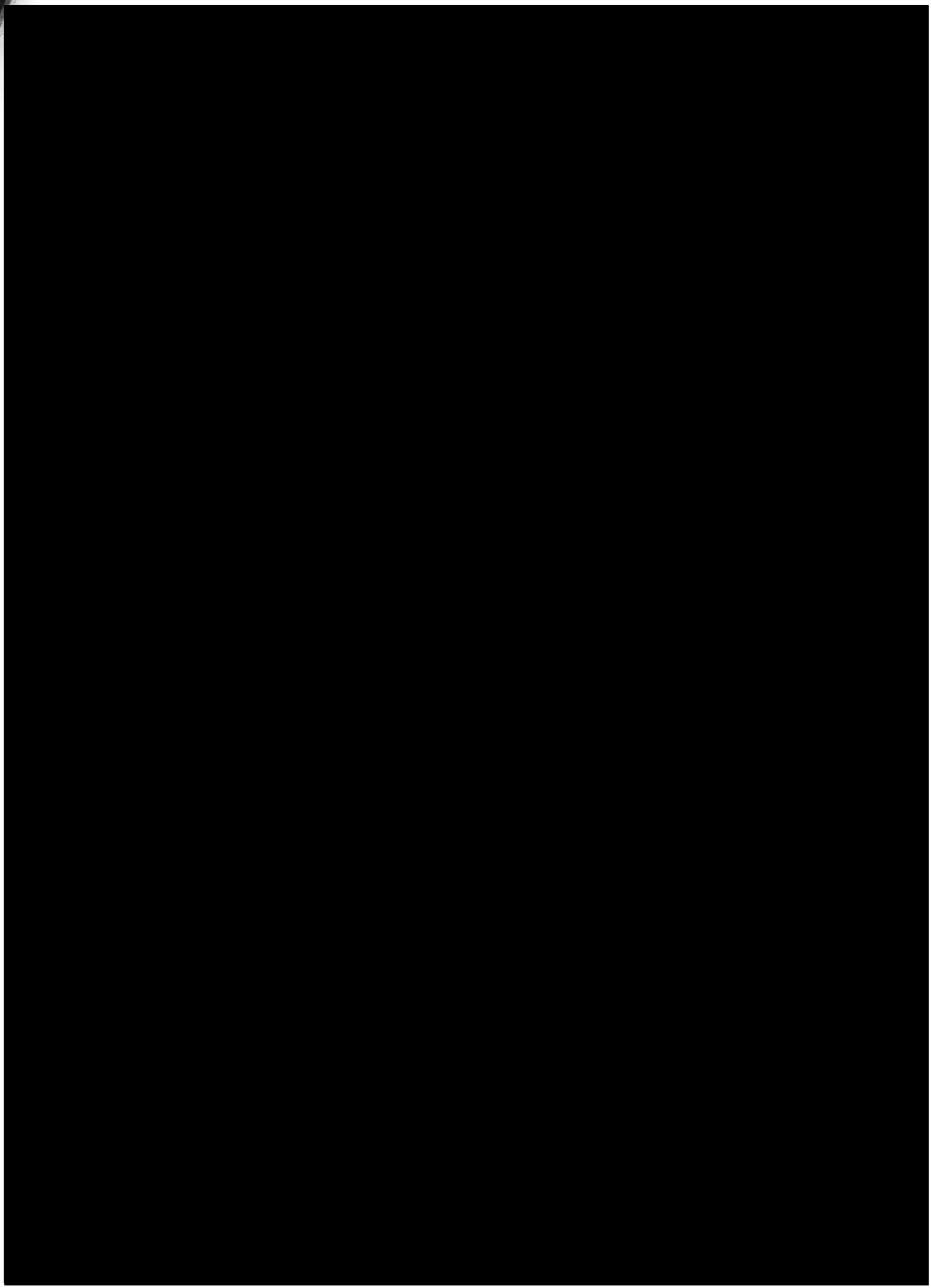


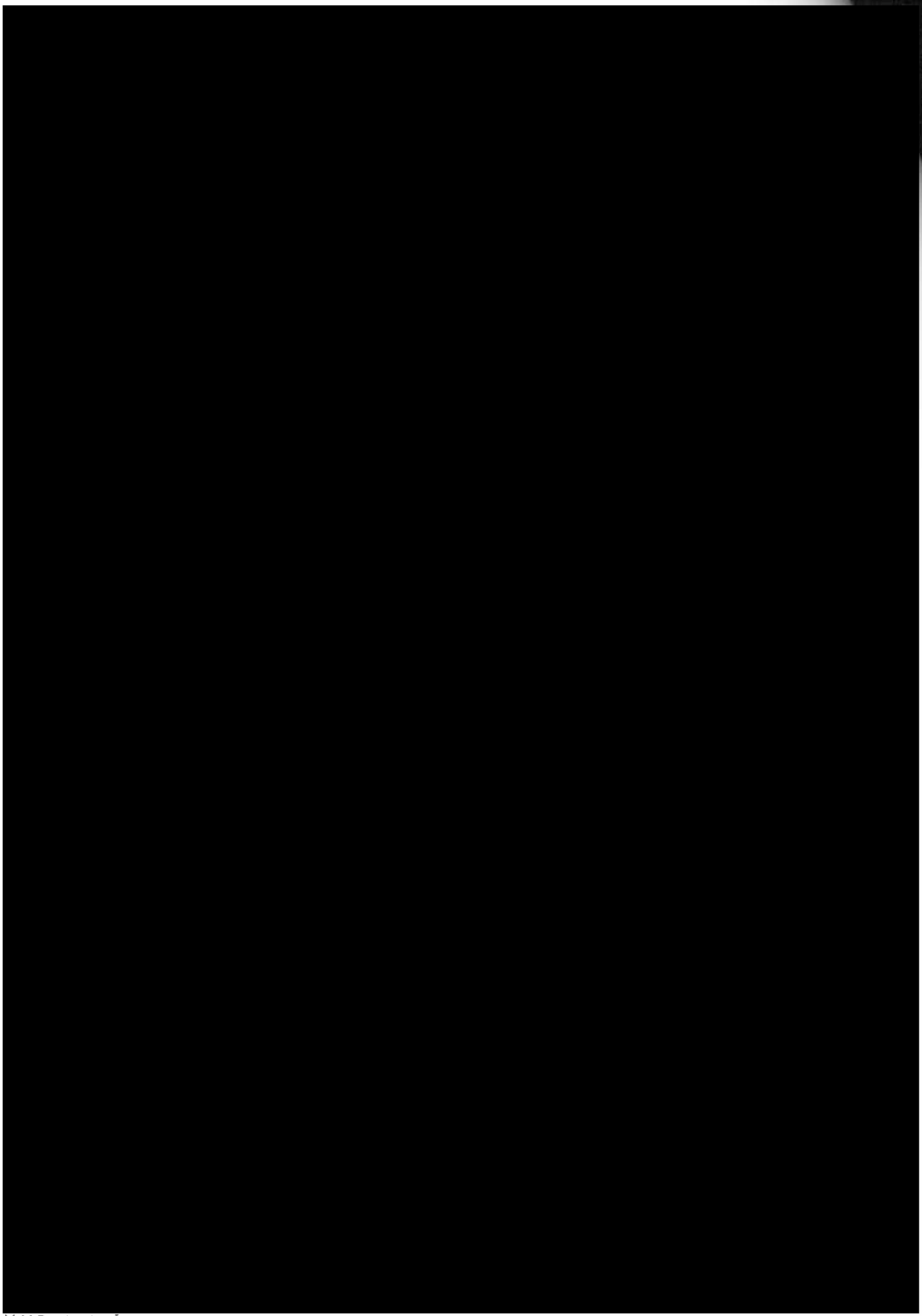


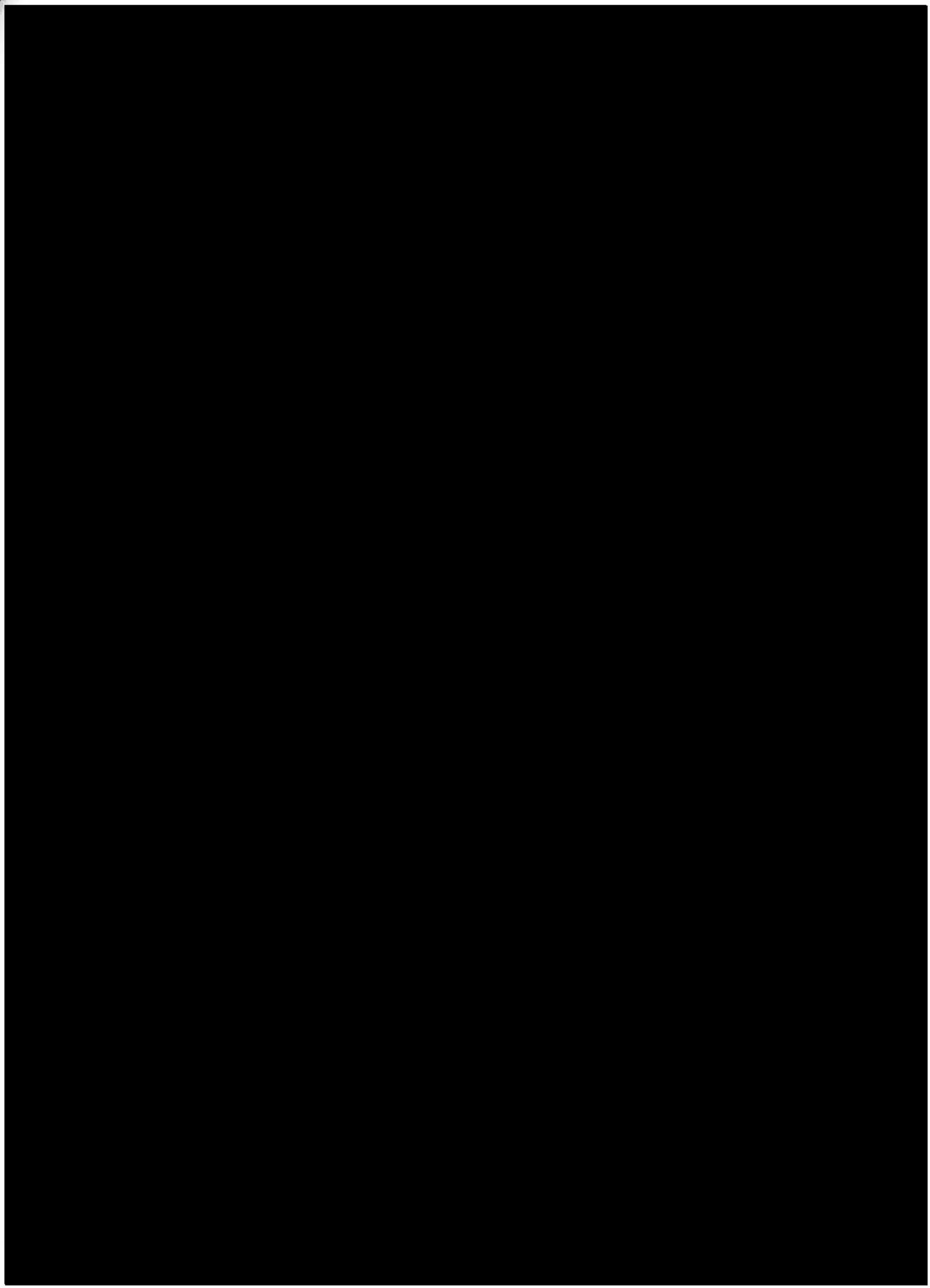


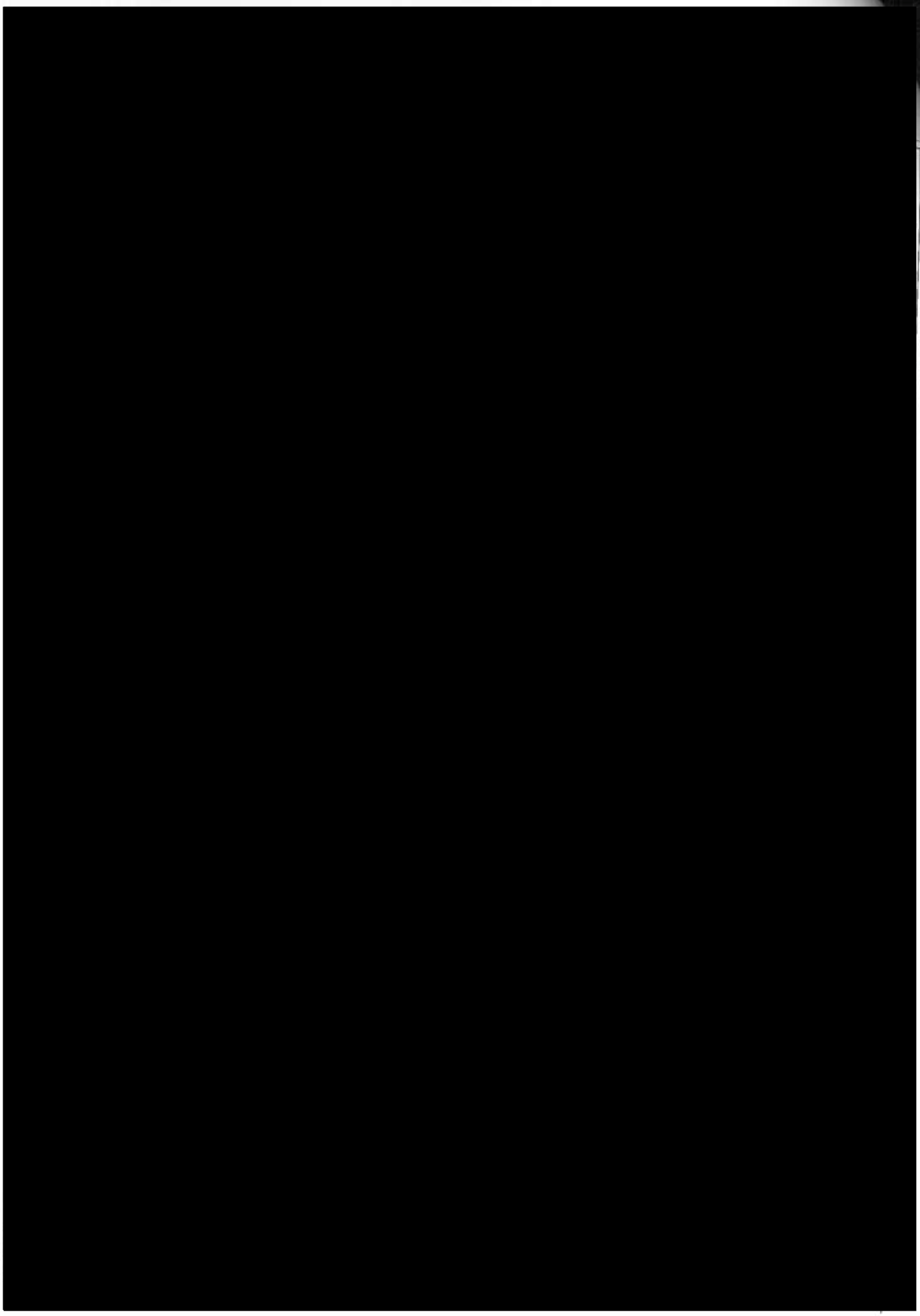


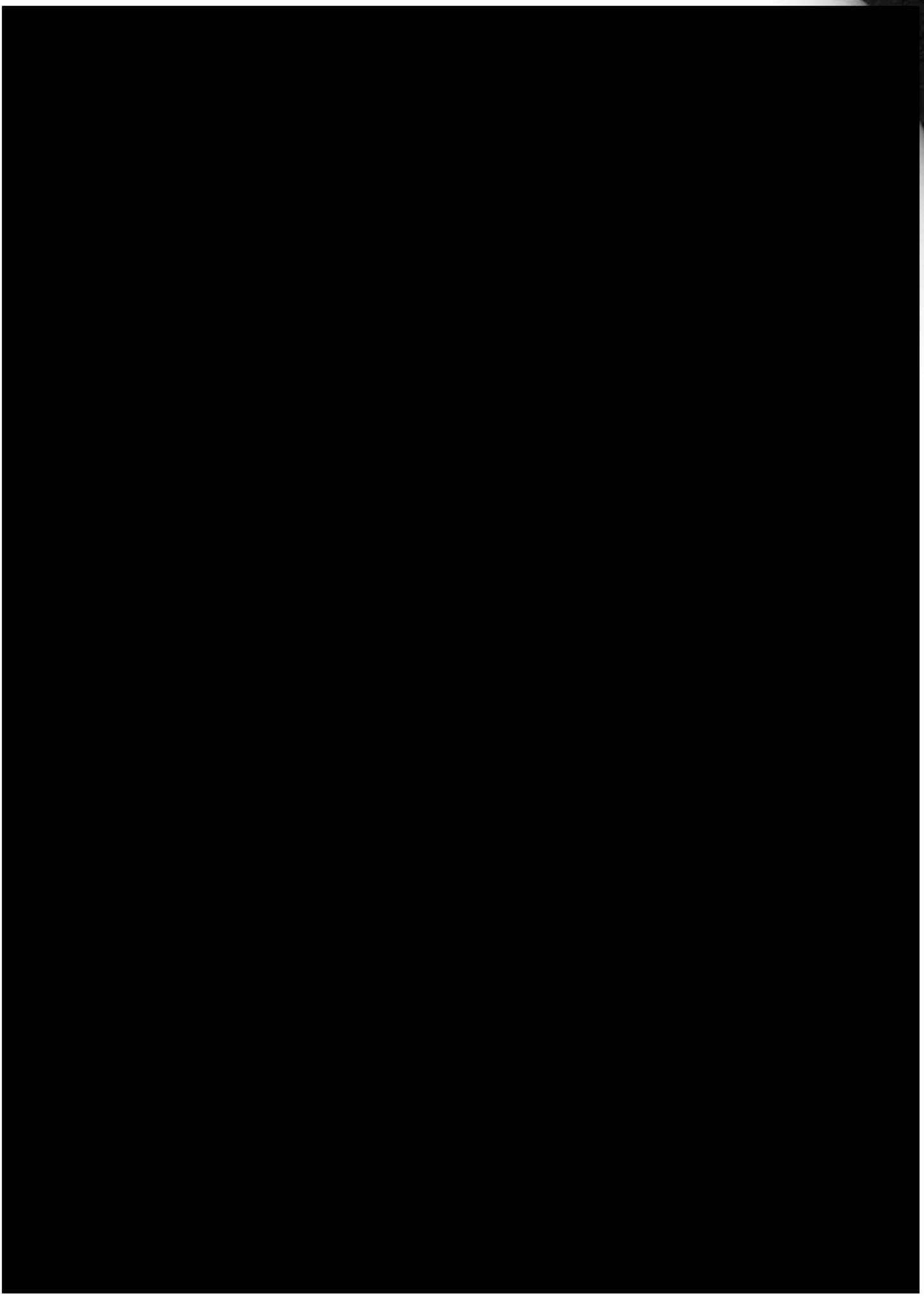


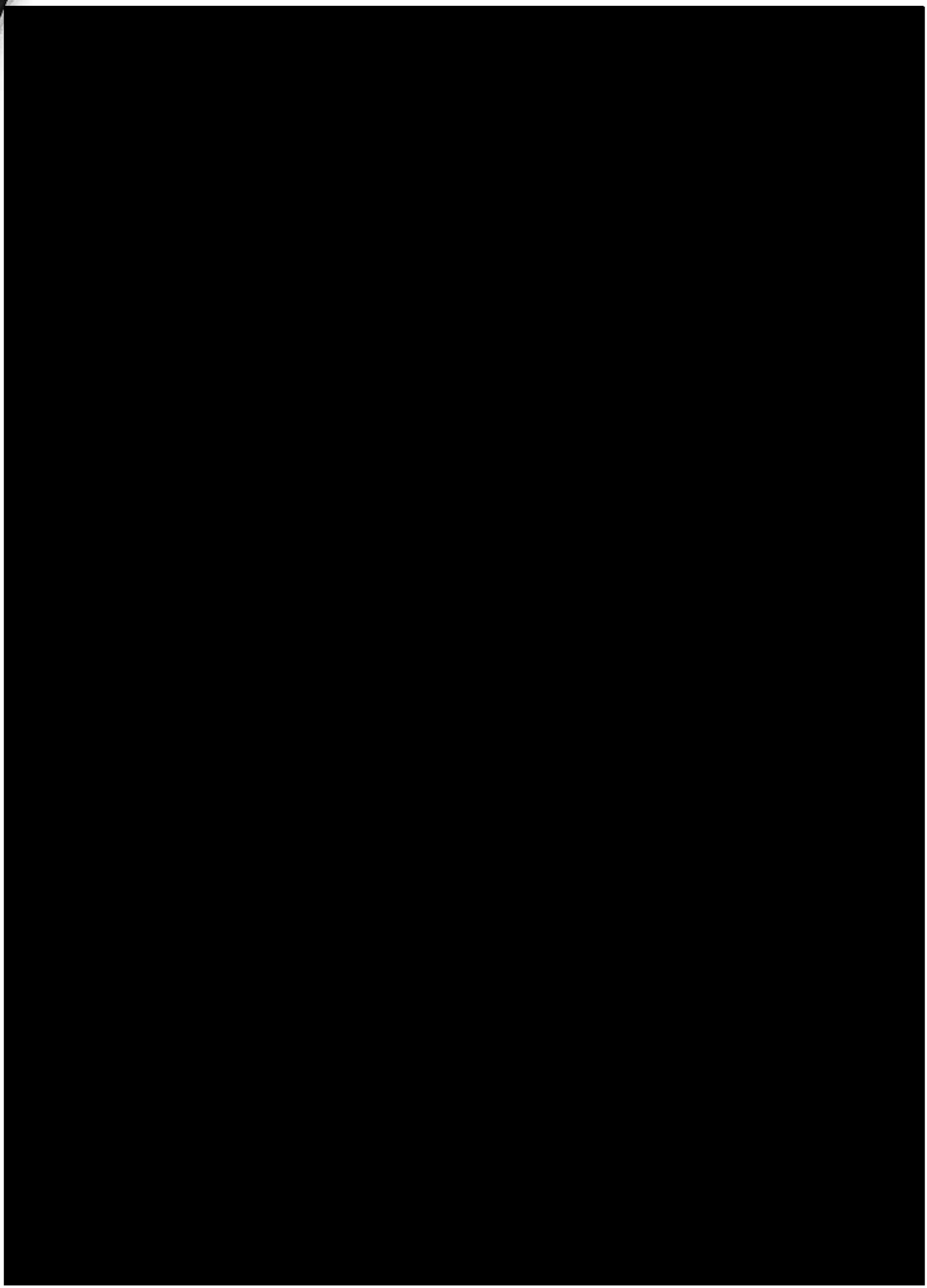












[redacted]

Příloha č. 2
k č. j. MV-112407-7/SSV-2016
počet listů 5

Příloha č. 4.2.2
Počet listů[1]: 10

Plán využití výsledků projektu a jejich popis[2]

Název/~~Jméno uchazeče~~: *)	Masarykova univerzita
Sídlo/~~Adresa uchazeče~~: *)	Žerotínovo náměstí 9, 601 77 Brno
IČ/~~RČ~~: *)	00216224
Název navrhovaného projektu:	Výzkum nástrojů pro hodnocení kybernetické situace a podporu rozhodování CSIRT týmů při ochraně kritické infrastruktury

Motivace k podání projektu (pouze jednu vhodnou variantu označte křížkem)

Projekt byl podán k vyřešení tržní nebo uživatelské potřeby	X
Projekt byl podán v reakci na tržní/kompetitivní výhodu	
Projekt byl podán ve snaze využít technického/vědeckého rozvoje	
Projekt byl podán v návaznosti na strategii managementu	

Důvody a podklady k motivaci

Hlavní důvody a motivace pro podání projektu vychází ze schválené Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. Zejména se jedná o prioritní oblast Ochrana národní KII a VIS. V rámci této oblasti jsou stanoveny v Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 následující cíle:

- Kontinuálně provádět analýzu a monitoring hrozeb a rizik v ČR – C.4.1 – Provádět sběr a analýzu informací o hrozbách a rizicích, a tím zajišťovat aktuální přehled o situaci v kybernetické bezpečnosti jak v ČR, tak i ve světě.
- Průběžně navyšovat odolnost, integritu a důvěryhodnost systémů a sítí KII a VIS – C.3.3 – Udržovat aktuální evidenci kybernetických bezpečnostních incidentů, vyhodnocovat je a navrhovat opatření.
- Zvyšovat národní možnosti, schopnosti a kapacity v oblasti aktivní obrany a protiopatření proti kybernetickým útokům – C.10.2 – Definovat soubor možných krizových situací a vytvářet krizové scénáře pro spolupráci, komunikaci a nasazení protiopatření v období krizových stavů.

Obsah opatření k zajištění kybernetické bezpečnosti stanovuje v návaznosti na zákon č. 181/2014 Sb. prováděcí vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, bezpečnostních incidentech, reaktivních opatřeních a stanovení náležitostí podání v oblasti kybernetické bezpečnosti.

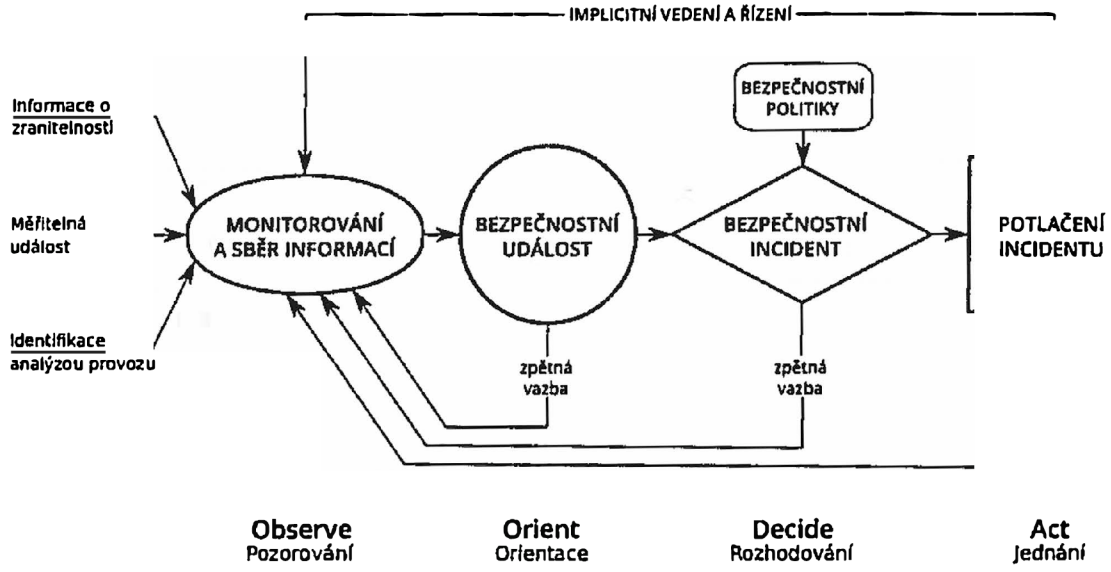
---

[1] *) Uchazeč záhlaví vyplní, nehodící se škrtněte
Uchazeč list vyplní, aktualizuje Počet listů

[2] Povinná příloha pro všechny uchazeče, v případě, že projekt podává více uchazečů, předkládá koordinátor

Prováděcí vyhláška uvádí technické prostředky, které jsou dnes dostupné správcům KII a VIS. Jedná se typicky o nástroje pro detekci, sběr a vyhodnocení bezpečnostních událostí. Správcům KII a VIS však schází nástroje pro komplexní hodnocení kybernetické situace (Situational Awareness), dále nástroje pro podporu rozhodování správců při ochraně KII a nástroje pro přijímání reaktivních opatření. V současné době jsou bezpečnostní incidenty řešeny často izolovaně bez ohledu na aktuální dění v síti. Rozhodování je plně v rukou správce, který musí správně vyhodnotit výstupy nástrojů pro vyhodnocení bezpečnostních událostí a na jejich základě navrhnout a nasadit vhodnou metodu obrany. Kvůli izolovanosti detekčních a reakčních systémů je však obtížné udržet komplexní informace o dění v KII. Mnohdy chybějící zpětná vazba od reaktivních opatření k dalším prvkům obrany KII pak může mít za následek chyby v rozhodování a může vést až k omezení dostupnosti prvků v KII.

Předkládaný projekt si proto klade za cíl zkoumat a vytvořit nástroje, které by rozšířili schopnosti stávajících technických prostředků. Činnosti správců (členů bezpečnostních týmů CSIRT) budou mapovány na rozhodovací proces cyklu OODA (Observe, Orient, Decide, Act), viz obr. 1., který představuje perspektivní způsob pro hodnocení kybernetické situace a podporu rozhodování členů CSIRT týmů.



Obr. 1. Rozhodovací proces založený na OODA cyklu.

Metodu OODA cyklu vytvořil John Boyd pro potřeby rozhodování v bojových operacích Leteckých sil Spojených států. V současnosti se jedná o uznávanou metodu pro efektivní reakci na události, která je používaná kromě vojenství i pro vysvětlení procesu učení, nebo rozhodovacích procesů v ekonomice.

Plánované výsledky projektu (4 x software) přispějí k plnění výše uvedených cílů akčního plánu a umožní hlubší a pokročilejší zajištění kybernetické bezpečnosti ČR.

Certifikace, zkoušky, testování a další nároky

Vytvořené nástroje budou průběžně testovány za simulovaných podmínek charakteristických pro budoucí operační nasazení. K testování bude využito prostředí Kybernetického polygonu (www.kypo.cz). Simulované komponenty KII budou obsahovat systémy pro detekci, sběr a

vyhodnocení bezpečnostních událostí. Po experimentálním ověření v Kybernetickém polygonu bude provedeno pilotní nasazení týmem CSIRT-MU na síti Masarykovy univerzity.

S ohledem na očekávanou koncovou úroveň vyspělosti výsledků projektu 5 (viz příloha č. 4.2.3), nejsou plánovány speciální certifikace vytvořených softwarových nástrojů. Při vývoji budou použity osvědčené postupy (best practices) používané při vývoji open-source bezpečnostních řešení. Zvolený přístup by neměl mít negativní vliv na potenciální uplatnění výsledků v praxi či jinak omezit jejich využití.

Předpokládaní uživatelé výsledků (křížkem označte pouze jeden tržní segment, ve kterém očekáváte **nejširší uplatnění** výsledků projektu)

Organizace s přímou odpovědností za zajišťování bezpečnosti (ozbrojené bezpečnostní sbory, záchranné sbory, SUJB, NBÚ, zpravodajské služby)	X
Organizace s regulatorní rolí v systému zajišťování bezpečnosti (ústřední správní úřady zastoupené v Bezpečnostní radě státu)	
Organizace zapojené do bezpečnostního systému ad hoc, nebo regulované krizovou legislativou (SBS, provozovatelé KI, vlastníci/provozovatelé KII, rizikové průmyslové provozy, samosprávy)	
Organizace bez zásadních kompetencí v oblasti zajišťování bezpečnosti a veřejnost (včetně výzkumných organizací u projektů směrovaných k dalšímu vývoji)	

Zdůvodnění určení uživatelů

Národní bezpečnostní úřad – v říjnu 2011 ustavila vláda České republiky Národní bezpečnostní úřad gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Národní bezpečnostní úřad tuto činnost zabezpečuje prostřednictvím Národního centra kybernetické bezpečnosti (NCKB), jehož součástí je Vládní CERT (GovCERT.CZ). Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům a přijímání opatření při řešení incidentů proti probíhajícím útokům. Výsledky projektu budou poskytnuty Vládnímu CERT a jemu podřízeným organizacím.

Ministerstvo obrany – v rámci resortu MO je Vojenské zpravodajství (VZ) pověřeno budováním Národního centra kybernetických sil (NCKS) a tomu odpovídajícím úkolům z Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. Další prvek kybernetické bezpečnosti resortu MO tvoří Centrum CIRC. Jeho úkolem je proaktivní identifikace bezpečnostních hrozeb a incidentů, jejich analýza a následné reportování zjištěných událostí a postupů řešení k relevantním partnerům. Výsledky projektu budou poskytnuty Centru CIRC a VZ.

Plánované záměry uchazeče v oblasti využití výsledku (pouze jednu vhodnou variantu označte křížkem)

Volné šíření	
Kontrolované nezpoplatněné šíření (registrace; smlouva; přímé předání, další vlastní využití ve VaV)	X
Kusový prodej	
Licenční prodej a/nebo prodej navazující služby	

Plánované záměry uchazeče v oblasti využití výsledků

Záměrem uchazeče je rozvíjet výsledky projektu tak, aby mohly být využity třetími stranami, zejména organizacemi s přímou odpovědností za bezpečnost státu (NBÚ, Ministerstvo vnitra, Ministerstvo obrany) a jim podřízeným organizacím. Výsledky budou zpřístupněny tak, aby jejich využívání nebylo v rozporu se zájmy České republiky a negativně neovlivňovalo bezpečnost České republiky a jejích občanů. Bezpečnostní tým uchazeče (CSIRT-MU) využije výsledky pro ochranu informačních a komunikačních systémů Masarykovy univerzity. V neposlední řadě budou výsledky využity a rozvíjeny v dalších VaV aktivitách uchazeče.

Vazba mezi uvedenými výsledky

Předpokládané výsledky projektu budou využitelné samostatně, nicméně integrální zapojení všech hlavních výstupů umožní plné využití klíčových vlastností cyklu OODA. Dílčí výsledky jsou mapovány na jednotlivé fáze OODA cyklu tak, aby pokryly všechny činnosti vyžadované implementací OODA cyklu v prostředí kybernetické bezpečnosti jak samostatně, tak i v rámci zpětné vazby mezi jednotlivými fázemi. Mezi jednotlivými výstupy budou definována komunikační rozhraní a formát výměny dat tak, aby bylo možné jednotlivé výsledky používat i ve spolupráci s dalšími nástroji. Díky tomu bude umožněna zaměnitelnost a rozšiřitelnost výsledků z hlediska reálného nasazení v existujících systémech a jejich další vývoj. Nástroje pro evidenci zranitelností a reaktivní obrany sítě mohou přispět ke zvýšení odolnosti sítě i samostatně. Nástroj pro podporu rozhodování pak najde své samostatné využití při výzkumu a simulaci bezpečnostních incidentů.

Zařazení projektu do příslušné kategorie[3] dle § 16 odst. 4 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: **„A"**

Uveďte jednotlivé plánované <u>hlavní výsledky</u> s těmito údaji:

Výsledek č. 1 – Software pro evidenci zranitelností v počítačové síti

- **Předběžný název a druh výsledku**

  Software pro evidenci zranitelností v počítačové síti – software (R)

- **Detailní popis výsledku**

  Výsledkem bude nástroj pro vyhledávání informací o zranitelnostech a evidenci zranitelných prvků komunikační infrastruktury. Systém bude odebírat informace o zranitelnostech, např. z databází CVE (Common Vulnerabilities and Exposures), NVD (National Vulnerability Database) nebo systémů pro sdíleni informací o bezpečnostních událostech (řešeno v projektech VI20152020026 a VI20162019029), a zjišťovat, které prvky v síti jsou danou zranitelností ohroženy. Ke zjišťování, zda se zranitelné prvky vyskytují v monitorované síti, budou využity metody pro pasivní i aktivní monitorování počítačových sítí a koncových zařízení. Počítá se s využitím a integrací existujících nástrojů, které jsou v sítích KII nasazeny. Nástroje pro pasivní monitorování umístěné na měřicích bodech budou vytvářet soupis aktivních prvků

[3] Uveďte písmeno a) až d) dle § 16 odst. 4 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.

v síti pomocí otisků (metoda fingerprintingu). V soupisu aktivních prvků pak budou vyhledávány potenciálně zranitelné systémy. Aktivní monitorovací nástroje budou sloužit k ověření výskytu zranitelnosti, pokud bude možné výskyt zranitelnosti automaticky otestovat. Výstupem nástroje bude soupis aktivních prvků v síti s vyznačením prvků zranitelných a potenciálně zranitelných. Soupis bude obsahovat informace o umístění a stavu měřicího bodu, zejména v případě rozmístění více měřicích bodů v síti. Výstupy budou obecně využitelné. V rámci projektu budou výstupy vytvořeného nástroje sloužit jako vstup pro software pro vizualizaci bezpečností situace v síti (Výsledek č. 2).

- **Přesná specifikace přínosů výsledku pro stávající bezpečnostní praxi**

  V mapování výstupu na rozhodovací cyklus OODA odpovídá výsledek fázi Observe. Výsledek umožní kontinuální sběr a analýzu informací o zranitelnostech a umožní evidenci výskytu zranitelností v monitorované síti. Automatizace procesu vyhledávání zranitelností umožní včas reagovat na možná ohrožení KII a odhadnout závažnost zranitelností pro danou síť. Stávající bezpečnostní praxí je práce nejméně se dvěma různými systémy, jednak se systémy pro monitorování komunikační infrastruktury a detekci bezpečnostních událostí, a poté se systémy pro sdílení informací o bezpečnostních událostech. Výsledek propojí dosud nepropojené oblasti, čímž urychlí vyhodnocení závažnosti situace a zjednoduší další postup řešení bezpečnostního incidentu. Administrátoři komunikačních infrastruktur nebudou muset aktivně sledovat hlášení o zranitelnostech a ručně vyhledávat zranitelné prvky infrastruktury, ale dostanou k dispozici automaticky generovaný soupis aktivních prvků v síti s vyznačením prvků zranitelných, případně potenciálně zranitelných.

- **Způsob a rozsah právní ochrany výsledku**

  K využití výsledku jiným subjektem bude nutné nabytí licence. Předpokládá se využití volných licencí používaných u open-source software. Bude-li to nutné bude výsledek chráněn tak, aby ho nebylo možné využít v rozporu s bezpečnostními zájmy České republiky.

- **Popis implementace výsledků**

  Výsledek bude využívat otevřenou architekturu a volně dostupné programové vybavení vhodným způsobem tak, aby aplikace výsledků do praxe a jejich používání nevyžadovalo nepřiměřené úsilí a dodatečné náklady.

- **Případný stupeň utajení výsledku dle zvláštních právních předpisů**[4]

  Výsledek nepodléhá žádnému stupni utajení dle zvláštních právních předpisů.

Výsledek č. 2 – Webová aplikace pro vizualizaci bezpečnostní situace v počítačové síti

- **Předběžný název a druh výsledku**

  Webová aplikace pro vizualizaci bezpečnostní situace v počítačové síti – software (R)

[4] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

- **Detailní popis výsledku**

  Výsledkem bude software pro vizualizaci aktuálního stavu počítačové sítě a systémů KII ve formě webové aplikace. Webový portál bude zobrazovat přehled o zabezpečení a dostupnosti kritických prvků informační infrastruktury. Dále bude vhodně vizualizovat data získaná z formálního popisu infrastruktury, monitorování a evidence zranitelností. Formální popis infrastruktury vychází z evidence prvků komunikační infrastruktury dodané jejím správcem se zřetelem na výskyt prvků KII. Uživateli bude v různých úrovních podrobnosti zobrazena zjednodušená topologie sítě, na které budou zvýrazněny zranitelné nebo nedostupné prvky kritické infrastruktury, vazby mezi prvky KII a prvky monitorovací infrastruktury. Kromě topologie bude portál zobrazovat informace o aktuálních zranitelnostech, historii bezpečnostních incidentů v dané síti a návrhy řešení probíhajících bezpečnostních incidentů. Prezentované informace budou přehledně strukturovány, aby se v nich uživatel snadno orientoval a nebyl zahlcen množstvím detailních informací.

  - Webový portál přehledně zobrazí kritickou infrastrukturu (logické celky systémů), jednotlivé prvky KII zobrazí v topologii sítě, ve které vyznačí zranitelné stroje na základě výstupů software pro evidenci zranitelností (Výsledek č. 1).
  - Pro usnadnění orientace v bezpečnostní situaci na síti bude systém zobrazovat informace o aktuálních zranitelnostech a historii bezpečnostních incidentů.
  - Portál bude nabízet postupy řešení bezpečnostních incidentů podle výstupů software pro podporu rozhodování (Výsledek č. 3) a možností adaptivní konfigurace sítě a monitorovací infrastruktury (Výsledek č. 4).

- **Přesná specifikace přínosů výsledku pro stávající bezpečnostní praxi**

  V mapování výstupu na rozhodovací cyklus OODA odpovídá výsledek fázi Orient. Orientace v aktuální situaci je klíčová pro správné řešení bezpečnostních incidentů. Systém bude v reálném čase poskytovat informace o dění v síti, což zkrátí dobu potřebnou pro zjištění závažnosti bezpečnostního incidentu a přípravu protiopatření. Vizualizace rozmístění prvků KII a vyznačení zranitelností v monitorované infrastruktuře pomůže rychlé orientaci v aktuální bezpečnostní situaci. Informace o historii bezpečnostních incidentů uživateli napoví, zda již podobný incident nastal a jak byl řešen, což napomůže rozhodování o dalším postupu řešení. V jedné webové aplikaci dojde k propojení informací o KII s topologií sítě, evidencí zranitelností a nabídkou možných reakcí na bezpečnostní incident.

- **Způsob a rozsah právní ochrany výsledku**

  K využití výsledku jiným subjektem bude nutné nabytí licence. Předpokládá se využití volných licencí používaných u open-source software. Bude-li to nutné bude výsledek chráněn tak, aby ho nebylo možné využít v rozporu s bezpečnostními zájmy České republiky.

- **Popis implementace výsledků**

  Výsledek bude využívat otevřenou architekturu a volně dostupné programové vybavení vhodným způsobem tak, aby aplikace výsledků do praxe a jejich používání nevyžadovalo nepřiměřené úsilí a dodatečné náklady.

- **Případný stupeň utajení výsledku dle zvláštních právních předpisů**[5]

  Výsledek nepodléhá žádnému stupni utajení dle zvláštních právních předpisů.

Výsledek č. 3 – Software pro podporu rozhodování při řešení bezpečnostního incidentu

- **Předběžný název a druh výsledku**

  Software pro podporu rozhodování při řešení bezpečnostního incidentu – software (R)

- **Detailní popis výsledku**

  Výsledkem bude software pro podporu rozhodování administrátora zodpovědného za řešení bezpečnostního incidentu. Systém bude zpracovávat informace o aktuální bezpečnostní situaci v komunikační infrastruktuře včetně hlášení o bezpečnostních incidentech. S pomocí vhodných matematických modelů budou vybrány optimální bezpečnostní opatření s ohledem na topologii sítě, rozmístění prvků aktivní obrany a požadavky na dostupnost, důvěrnost a integritu prvků KII. Ty pak mohou být rozhodující osobě zobrazeny například ve webové aplikaci pro vizualizaci bezpečnostní situace (Výsledek č. 2). Navrhované opatření bude vybaveno vahou, vyjadřující nakolik systém doporučuje tuto akci provést, a informacemi relevantními k rozhodnutí. Tyto informace budou obsahovat například kroky útočníka, které systém vyhodnotil jako nejvíce pravděpodobné, odhad škod, jaké může útočník v síti způsobit, a návrh opatření k potlačení útoku.

  Rozhodovací algoritmus bude při výběru bezpečnostního opatření do svého rozhodnutí zahrnovat následující faktory:

  - Škody, které útočník v síti způsobil či může v budoucnu způsobit.
  - Jak bezpečnostní opatření může ovlivnit požadavky na dostupnost, důvěrnost, důvěryhodnost a integritu chráněných systémů.
  - Jaký dopad bude mít bezpečnostní opatření na legitimní uživatele a závislé služby a jestli případná opatření nenaruší běžný provoz v síti.

  Systém bude umožňovat, aby správce KII mohl do výstupu promítnout expertní názor. Správce zadá, jakou akci by zvolil, a nakolik si je danou volbou jistý. Systém na základě tohoto vstupu přehodnotí navrhovaná bezpečnostní opatření a vytvoří novou sadu návrhů, která vznikne kombinací výsledků matematického modelu a vstupů od správce KII.

- **Přesná specifikace přínosů výsledku pro stávající bezpečnostní praxi**

  V mapování výstupu na rozhodovací cyklus OODA odpovídá výsledek fázi Decide. Výsledek přispěje ke zvýšení a zkvalitnění kapacit pro aktivní obranu před kybernetickými útoky. Podpora rozhodování přispěje ke zlepšení kvality řešení bezpečnostních incidentů předzpracováním informací (např. odhadem škod) a

[5] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

redukcí počtu chyb zaviněných lidským faktorem. Díky předzpracování informací je možné rychleji reagovat na vzniklou situaci a dříve tak zabránit možným škodám. Za účelem redukce chyb může být výstup systému pro podporu rozhodování použit jako varování před kroky, které by mohly narušit dostupnost legitimních služeb (např. prvků KII) nebo plynulost síťového provozu. Výsledek umožní zkombinovat analytické rozhodování založené na matematických modelech s intuitivním rozhodováním založeném na zkušenosti.

- **Způsob a rozsah právní ochrany výsledku**

  K využití výsledku jiným subjektem bude nutné nabytí licence. Předpokládá se využití volných licencí používaných u open-source software. Bude-li to nutné bude výsledek chráněn tak, aby ho nebylo možné využít v rozporu s bezpečnostními zájmy České republiky.

- **Popis implementace výsledků**

  Výsledek bude využívat otevřenou architekturu a volně dostupné programové vybavení vhodným způsobem tak, aby aplikace výsledků do praxe a jejich používání nevyžadovalo nepřiměřené úsilí a dodatečné náklady.

- **Případný stupeň utajení výsledku dle zvláštních právních předpisů**[6]

  Výsledek nepodléhá žádnému stupni utajení dle zvláštních právních předpisů.

Výsledek č. 4 – Software pro aplikaci reaktivních opatření na prvcích aktivní obrany počítačové sítě

- **Předběžný název a druh výsledku**

  Software pro aplikaci reaktivních opatření na prvcích aktivní obrany počítačové sítě – software (R)

- **Detailní popis výsledku**

  Výsledkem bude software pro adaptivní konfiguraci prvků aktivní obrany komunikační infrastruktury. Software bude na základě popisu použitých technologií a metod pro analýzu síťového provozu určovat optimální varianty konfigurace prvků aktivní obrany. Software zpřístupní informace o aktuální konfiguraci a zátěži prvků monitorovací infrastruktury a zároveň umožní automaticky rekonfigurovat použité nástroje na základě doporučovaných reaktivních opatření. Možnosti analýzy provozu budou rozšířeny pomocí dostupných nástrojů pro přesměrování provozu. Přesměrovaný provoz bude možné analyzovat na prvcích s volným výpočetním výkonem, případně přesměrovat na specializovaný prvek pro daný úkon. Zároveň bude možné přesměrováním znemožnit útočníkovi další postup.

  Konfigurace reaktivních opatření na prvcích aktivní obrany bude sledovat jeden ze tří možných scénářů:

[6] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

- Zpřesnění analýzy síťového provozu beze změny směrování dat v síti.
- Změna směrování dat v síti za účelem přesměrování provozu na prvky aktivní obrany.
- Manipulace se síťovým provozem na prvcích aktivní obrany sítě.

V prvním případě jde o přenastavení měřicího bodu v síti tak, aby podrobněji analyzoval data, která jsou již přes daný prvek směrována. V druhém případě dochází k manipulaci síťového provozu tak, aby zájmový provoz protékal vybraným prvkem aktivní obrany, na kterém je dostupný vhodný nástroj pro zpracování daného provozu. Ve třetím případě jde o práci se síťovým provozem s cílem zájmový provoz blokovat, omezovat či přesměrovat mimo prvky KII.

- **Přesná specifikace přínosů výsledku pro stávající bezpečnostní praxi**

V mapování výstupu na rozhodovací cyklus OODA odpovídá výsledek fázi Act. Vložení dodatečných informací do rozhodovacího procesu umožní kontinuální optimalizaci spuštěných instancí metod pro analýzu provozu. Automatizované přenastavení těchto prvků umožní rychlejší a jednodušší úpravu monitorování a analýzy zájmového provozu. Zpřesňování informací získaných o provozu dále umožní lepší vyhodnocení a volbu reaktivních opatření.

- **Způsob a rozsah právní ochrany výsledku**

K využití výsledku jiným subjektem bude nutné nabytí licence. Předpokládá se využití volných licencí používaných u open-source software. Bude-li to nutné bude výsledek chráněn tak, aby ho nebylo možné využít v rozporu s bezpečnostními zájmy České republiky.

- **Popis implementace výsledků**

Výsledek bude využívat otevřenou architekturu a volně dostupné programové vybavení vhodným způsobem tak, aby aplikace výsledků do praxe a jejich používání nevyžadovalo nepřiměřené úsilí a dodatečné náklady.

- **Případný stupeň utajení výsledku dle zvláštních právních předpisů**[7]

Výsledek nepodléhá žádnému stupni utajení dle zvláštních právních předpisů.

[7] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

[redacted]

Datum podpisu	9. prosince 2015
Místo podpisu	Brno
Otisk razítka uchazeče	[redacted]
Jméno, příjmení a podpis uchazeče, resp. statutárního zástupce uchazeče	doc. PhDr. Mikuláš Bek, Ph.D. [redacted]