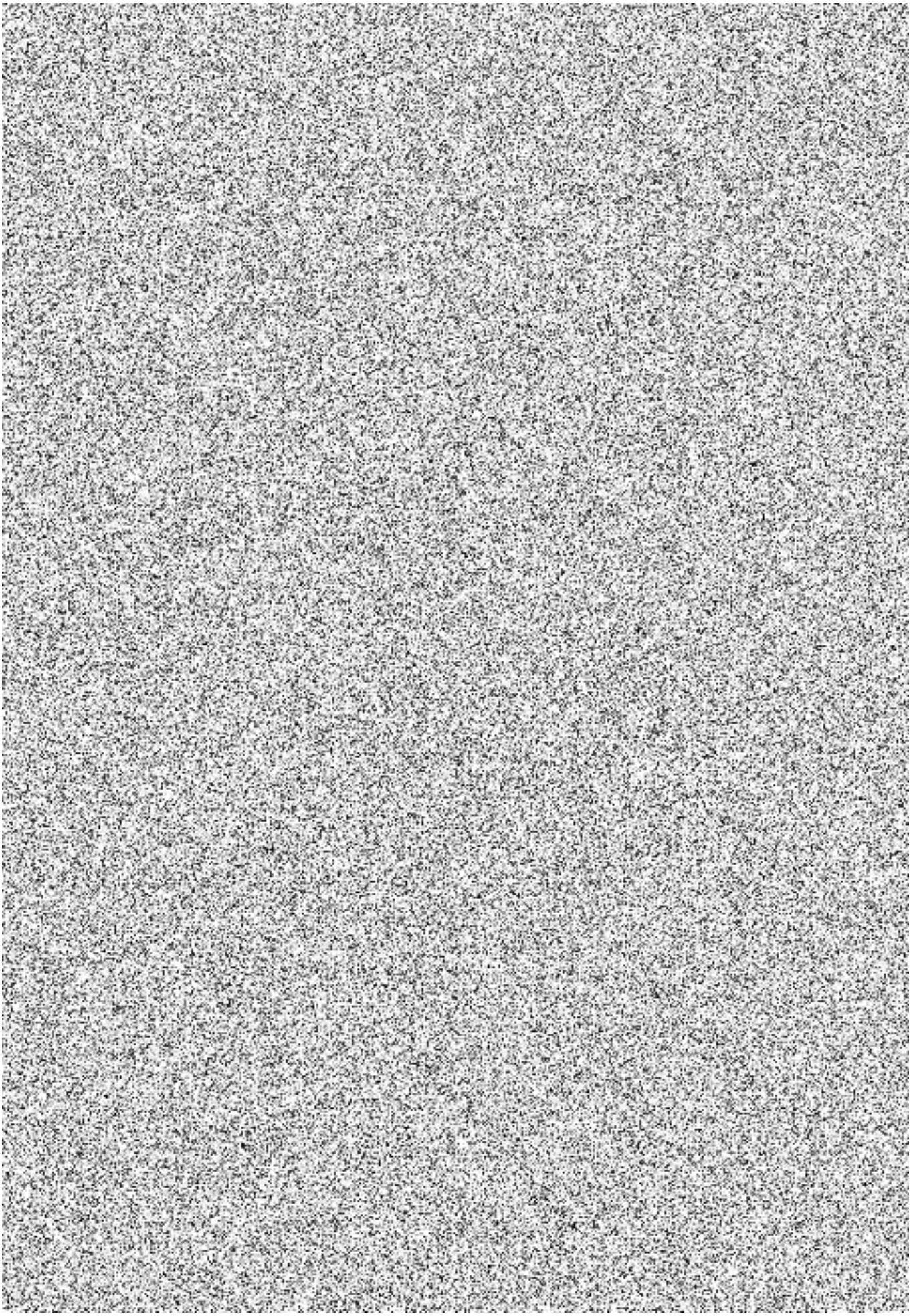
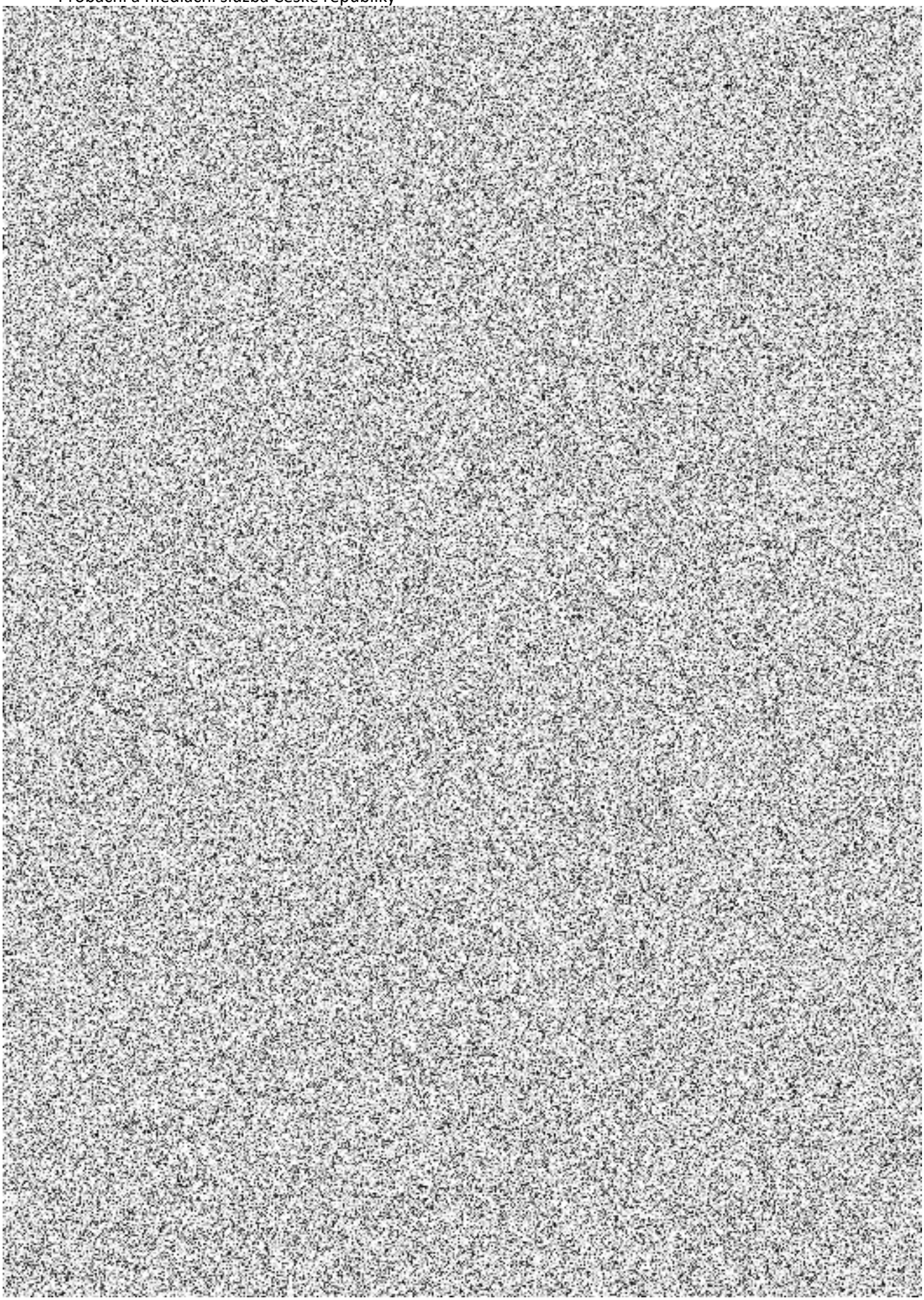
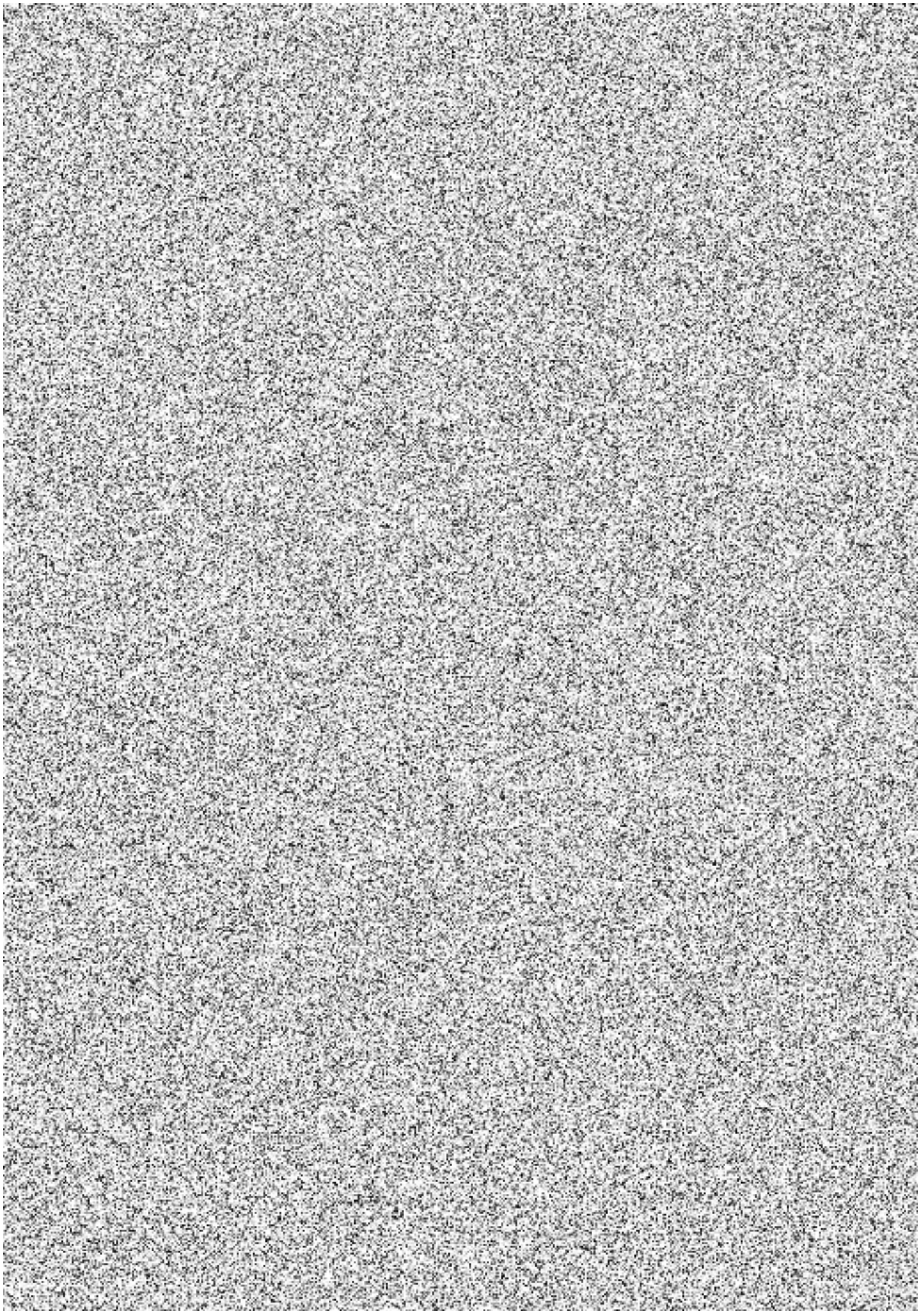
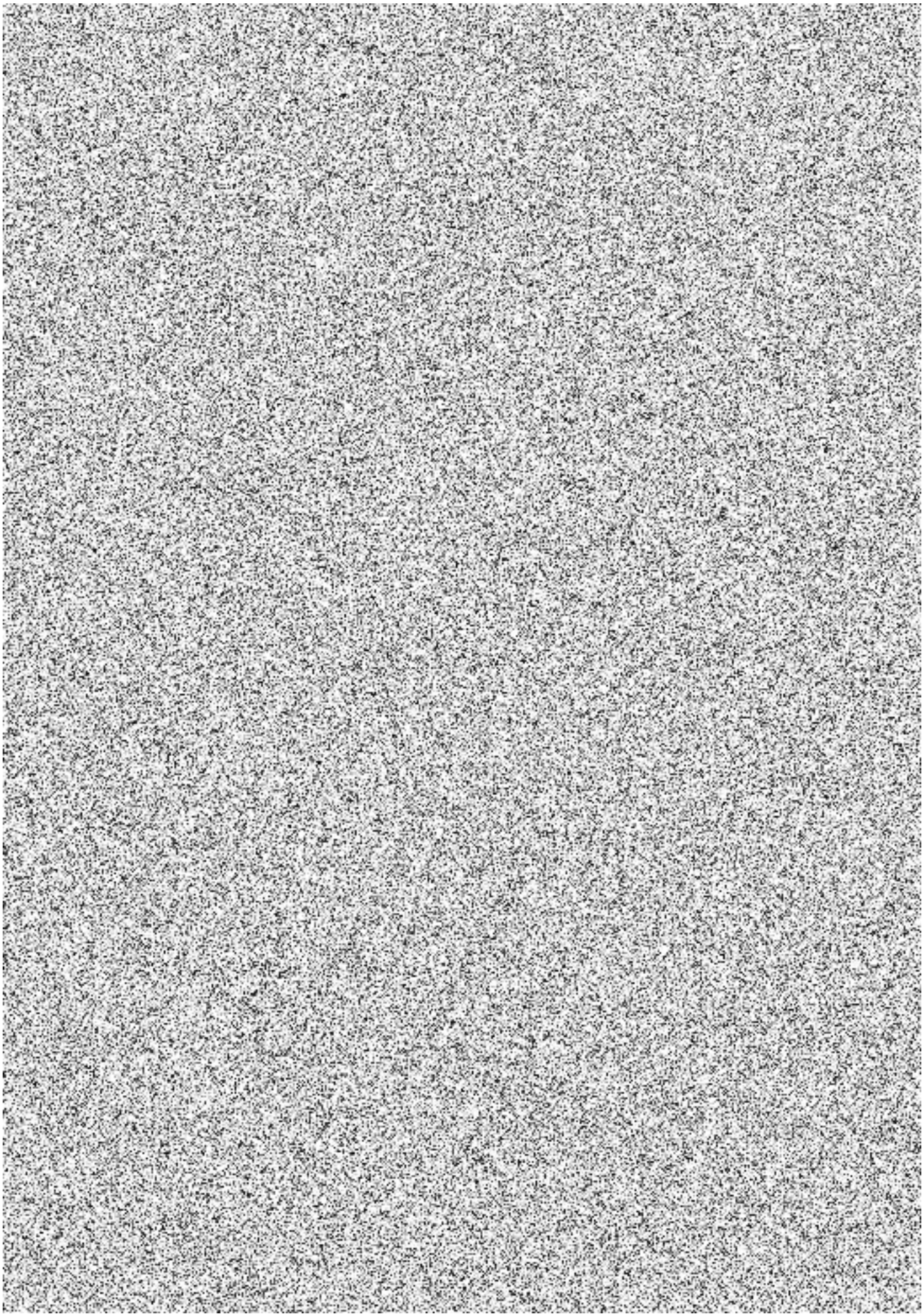
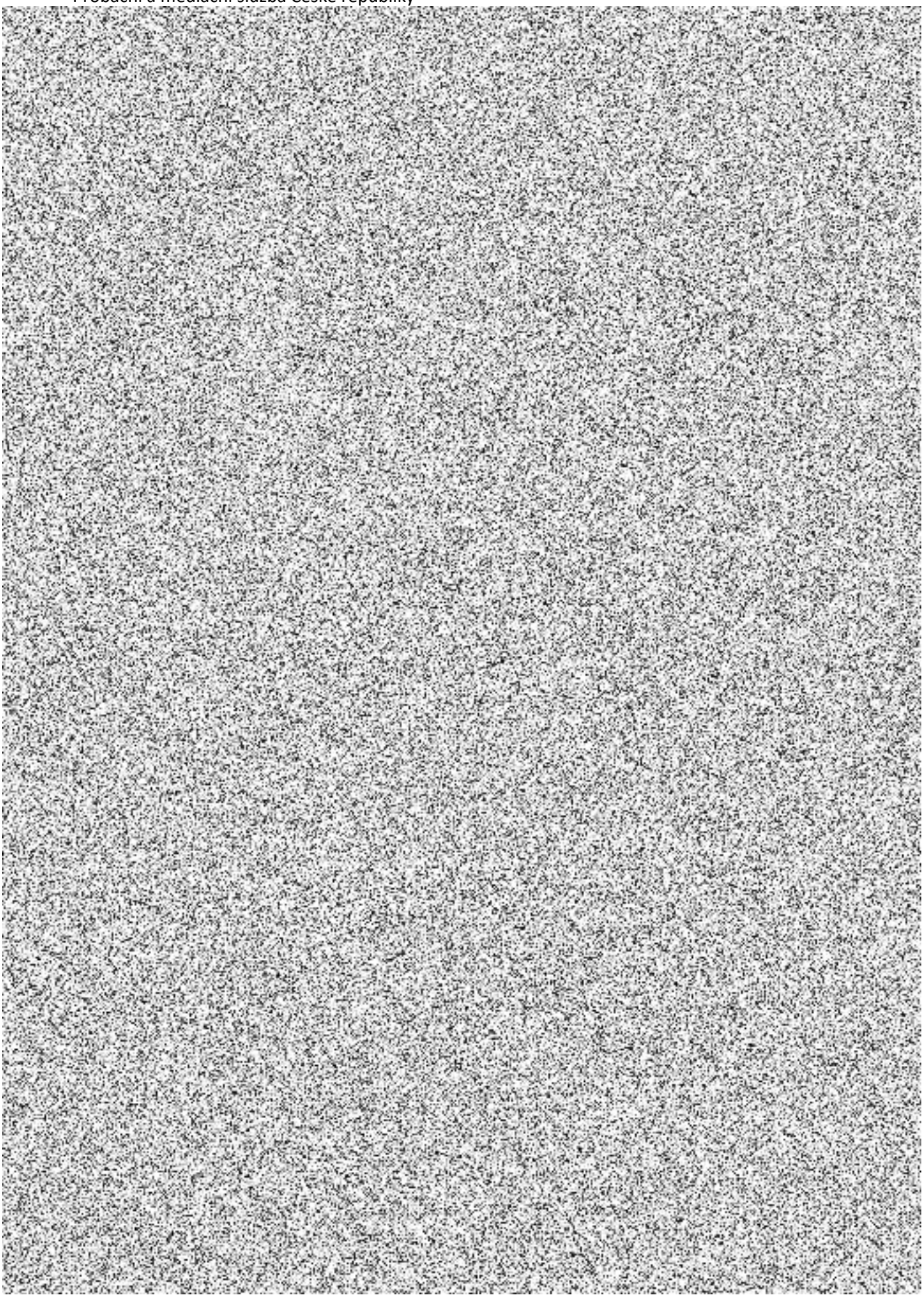
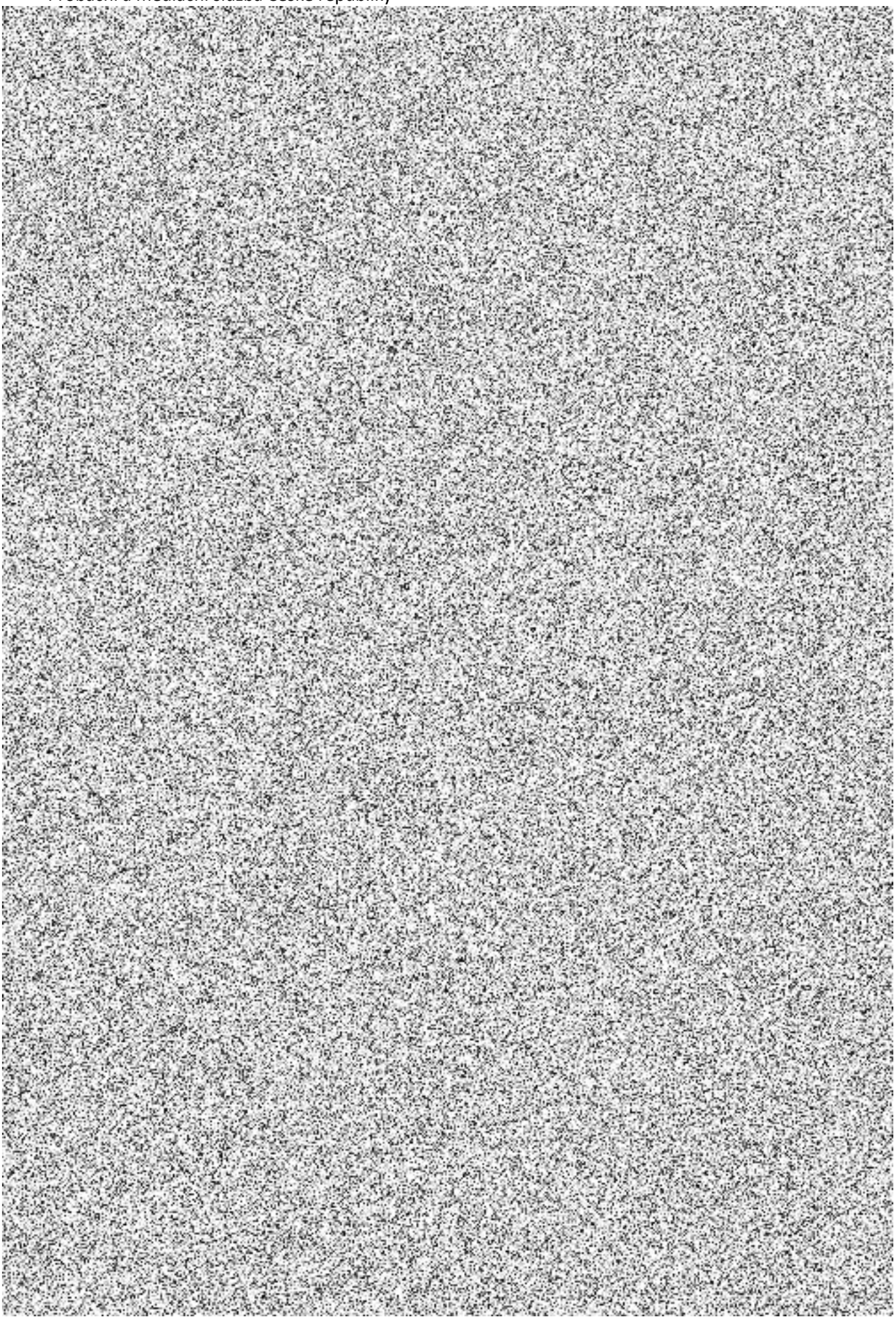


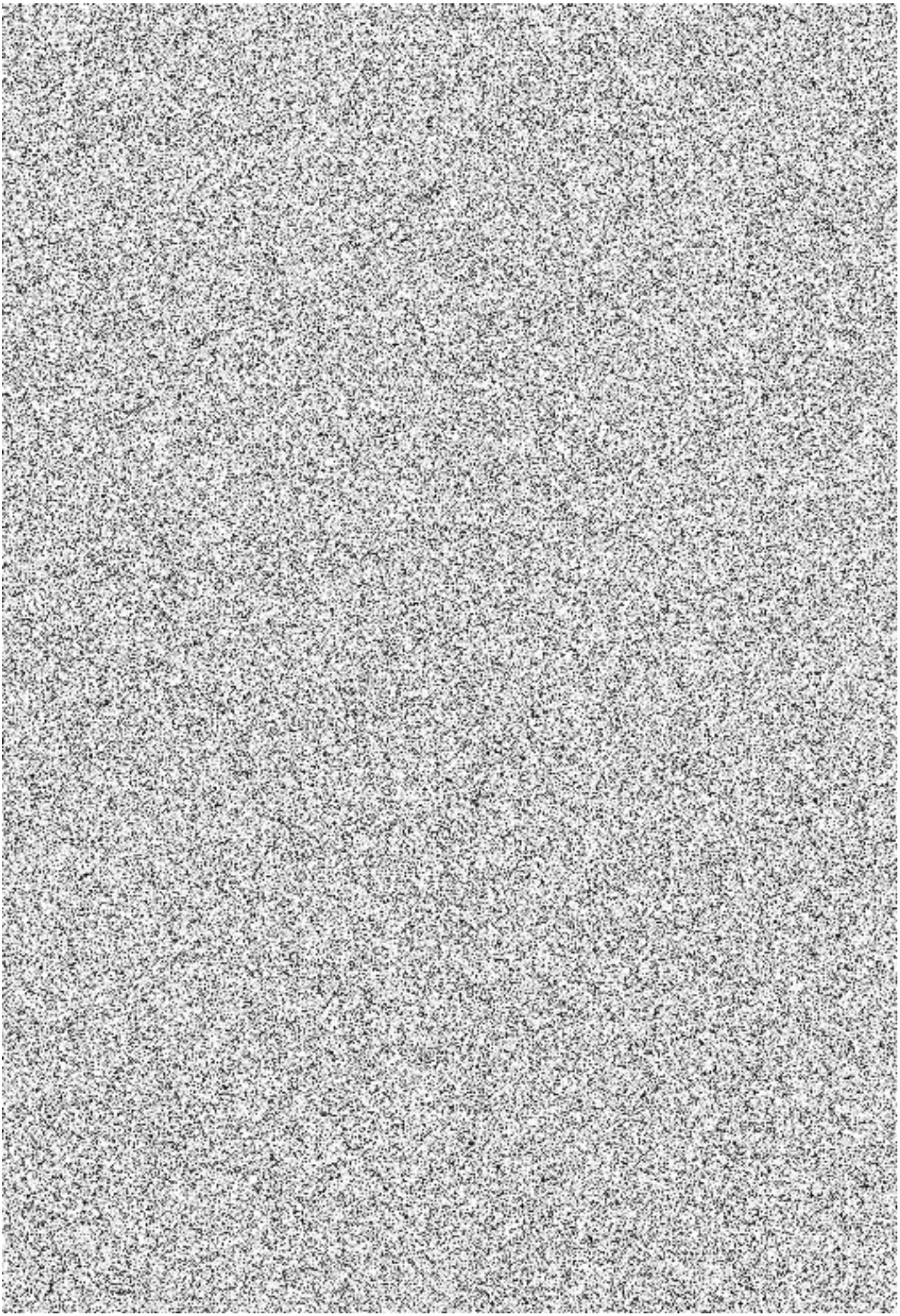


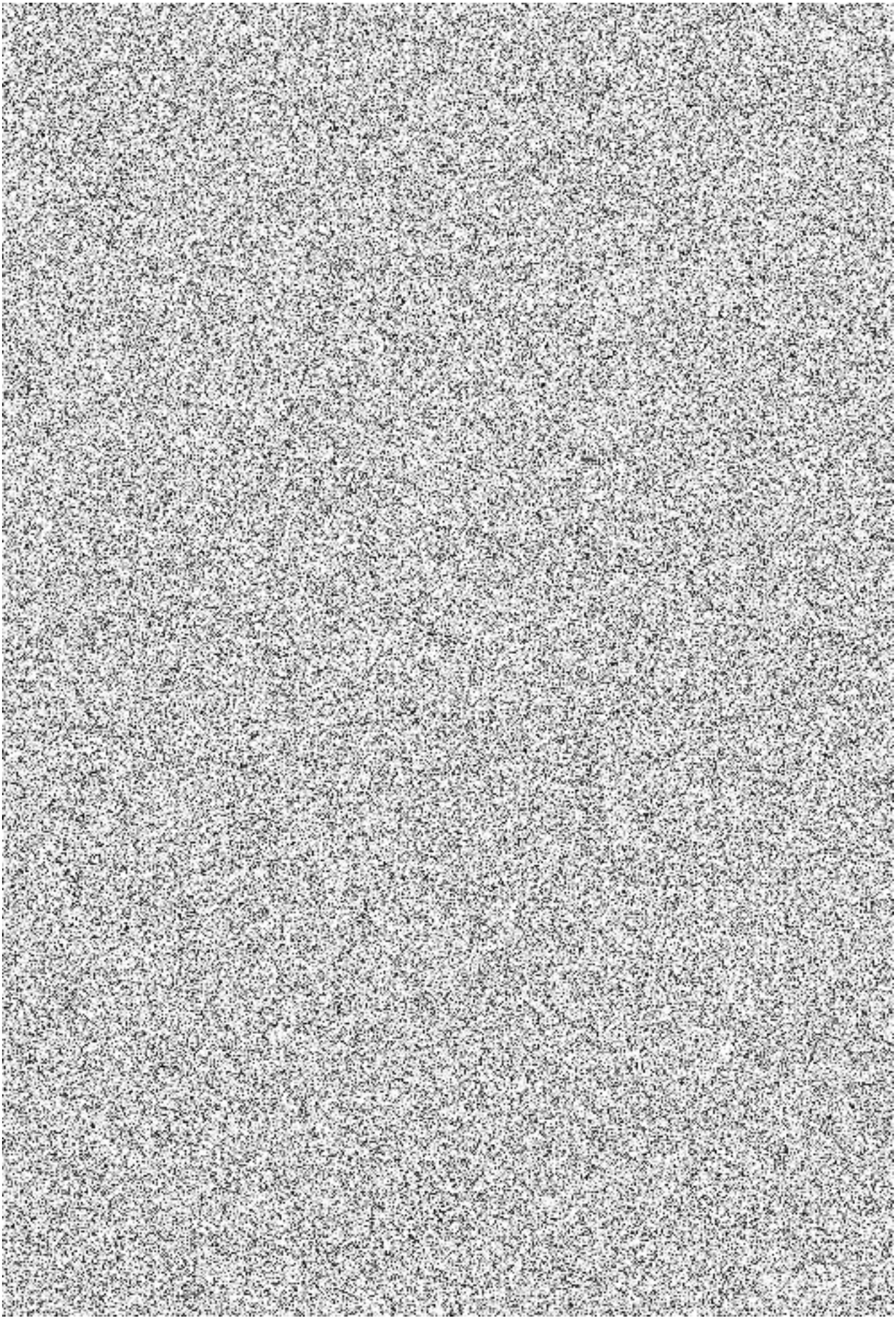


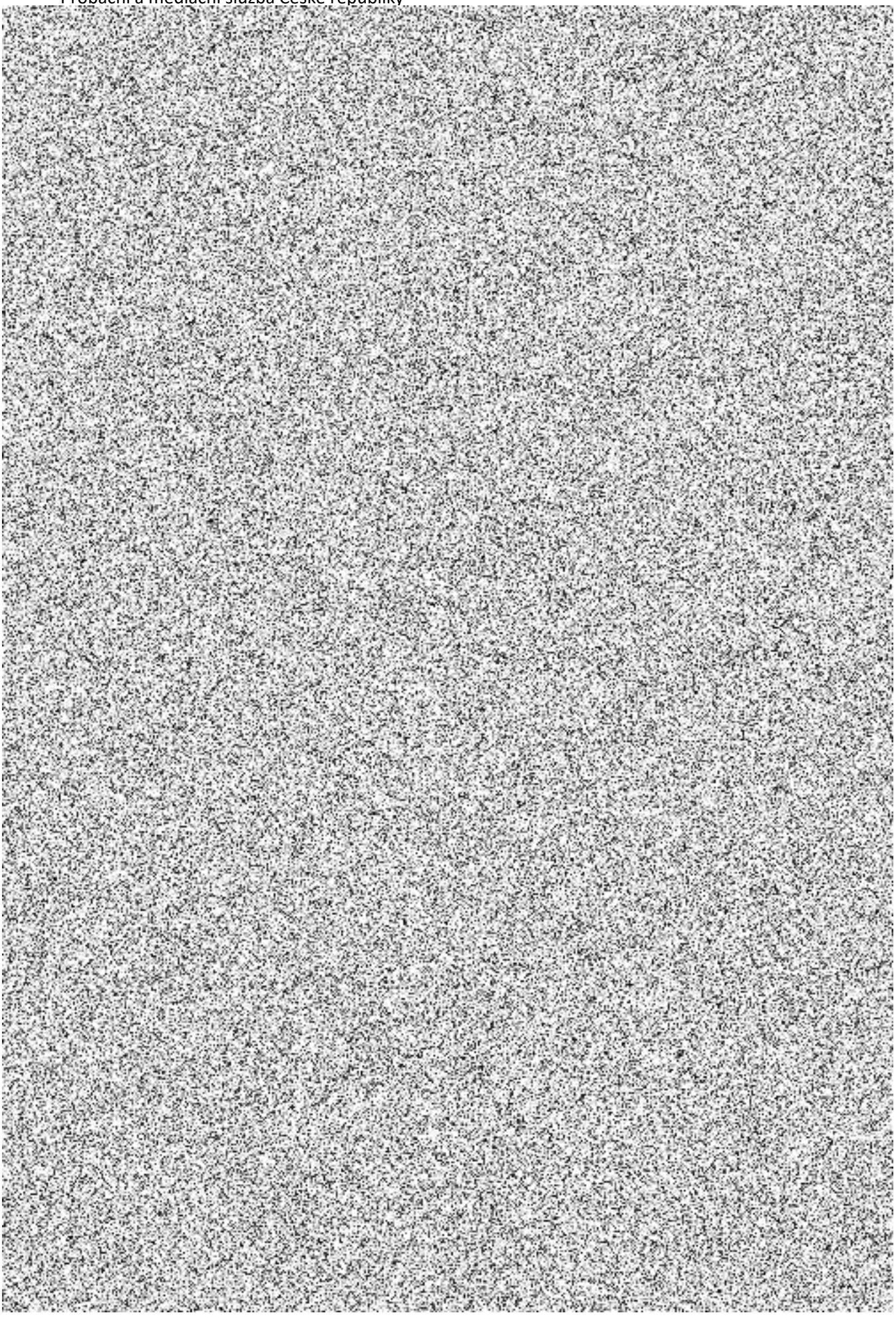


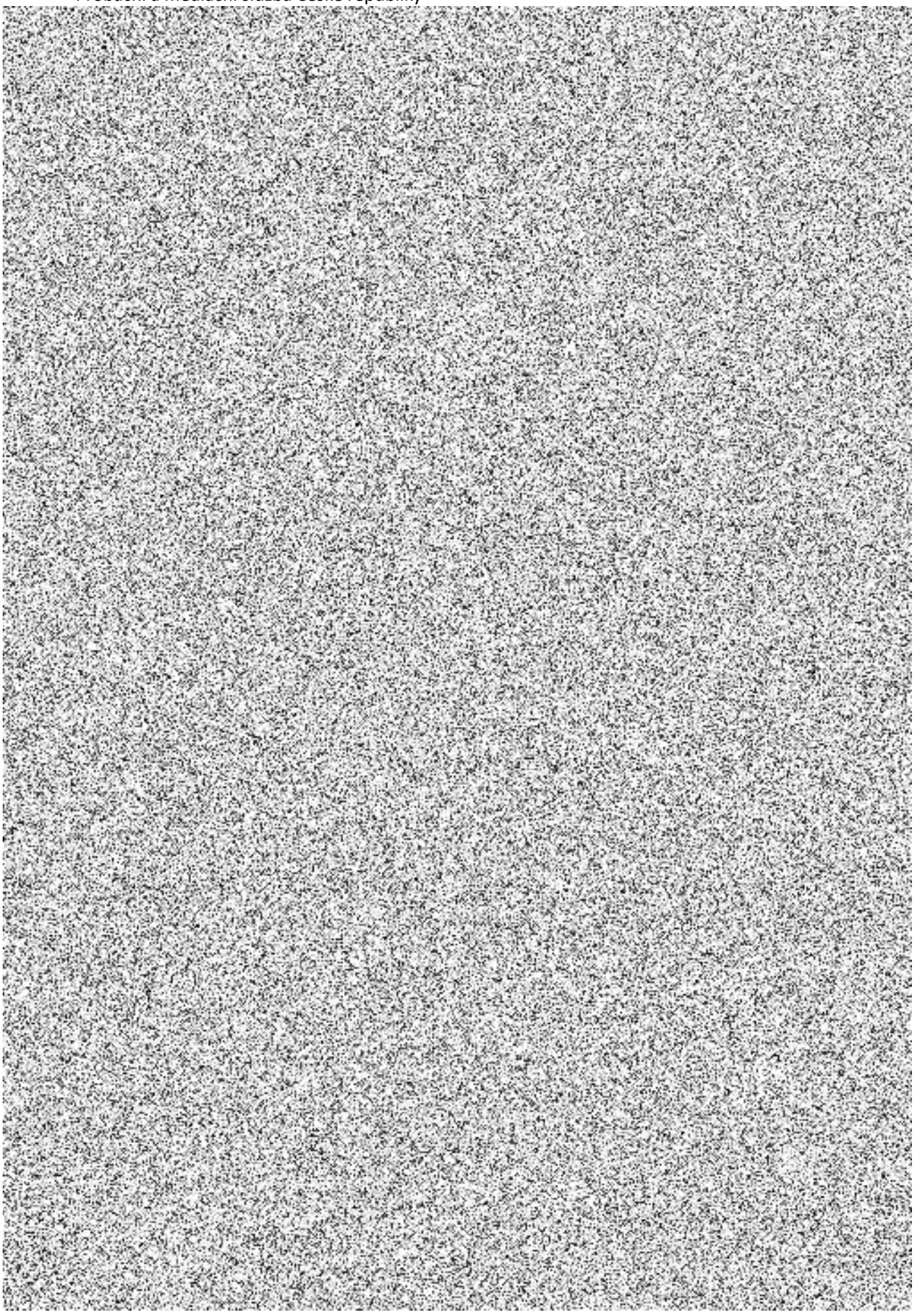


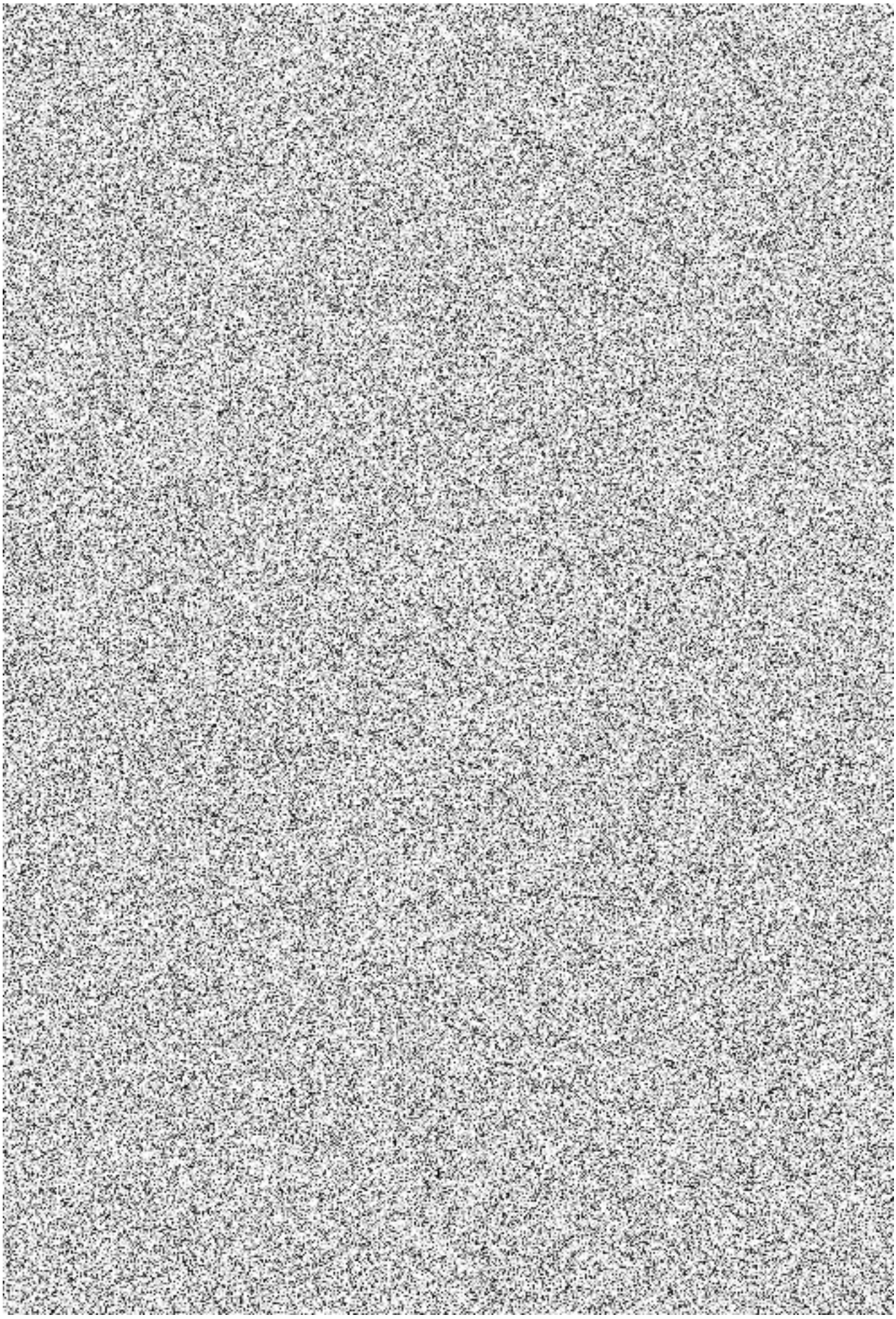


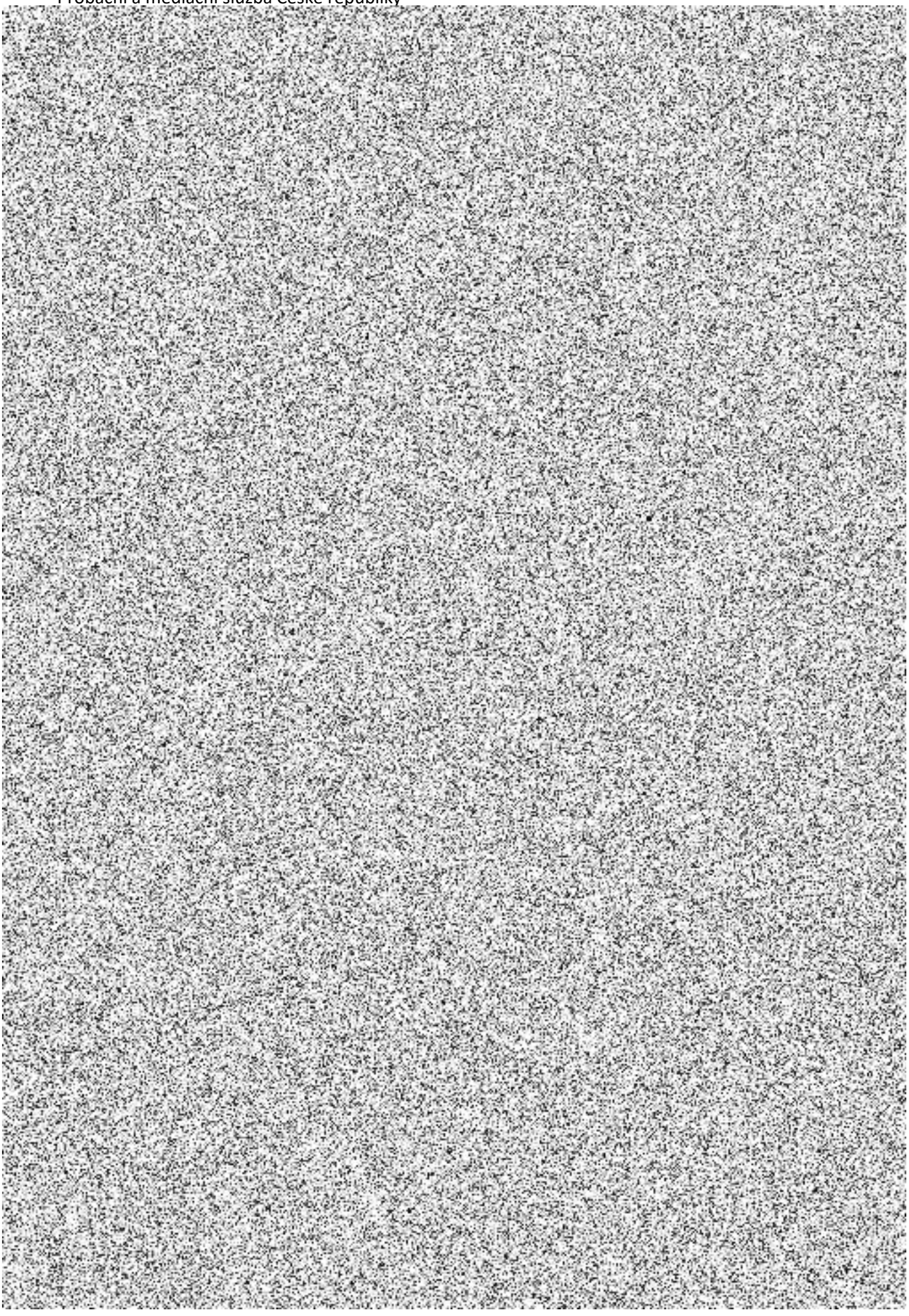


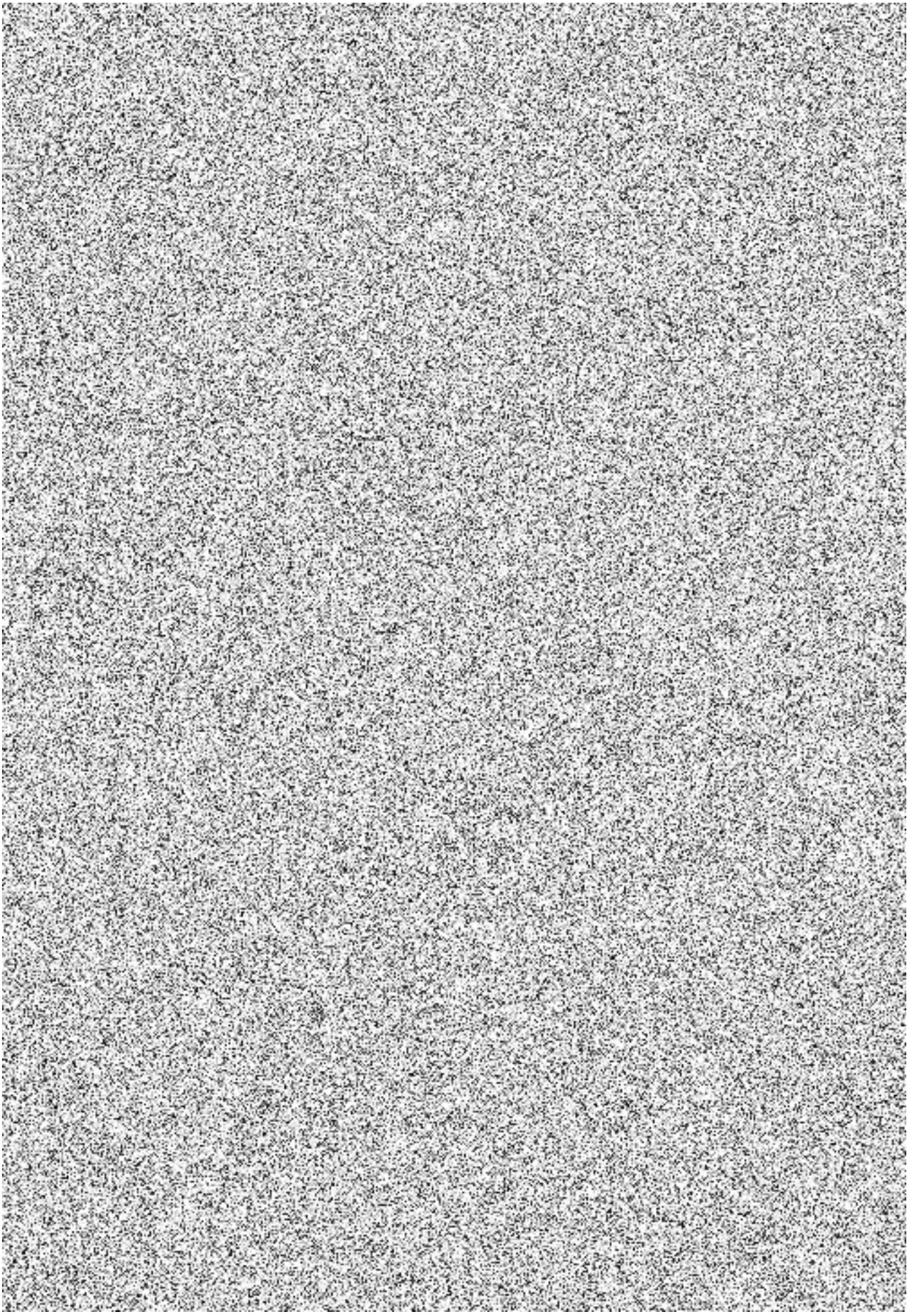


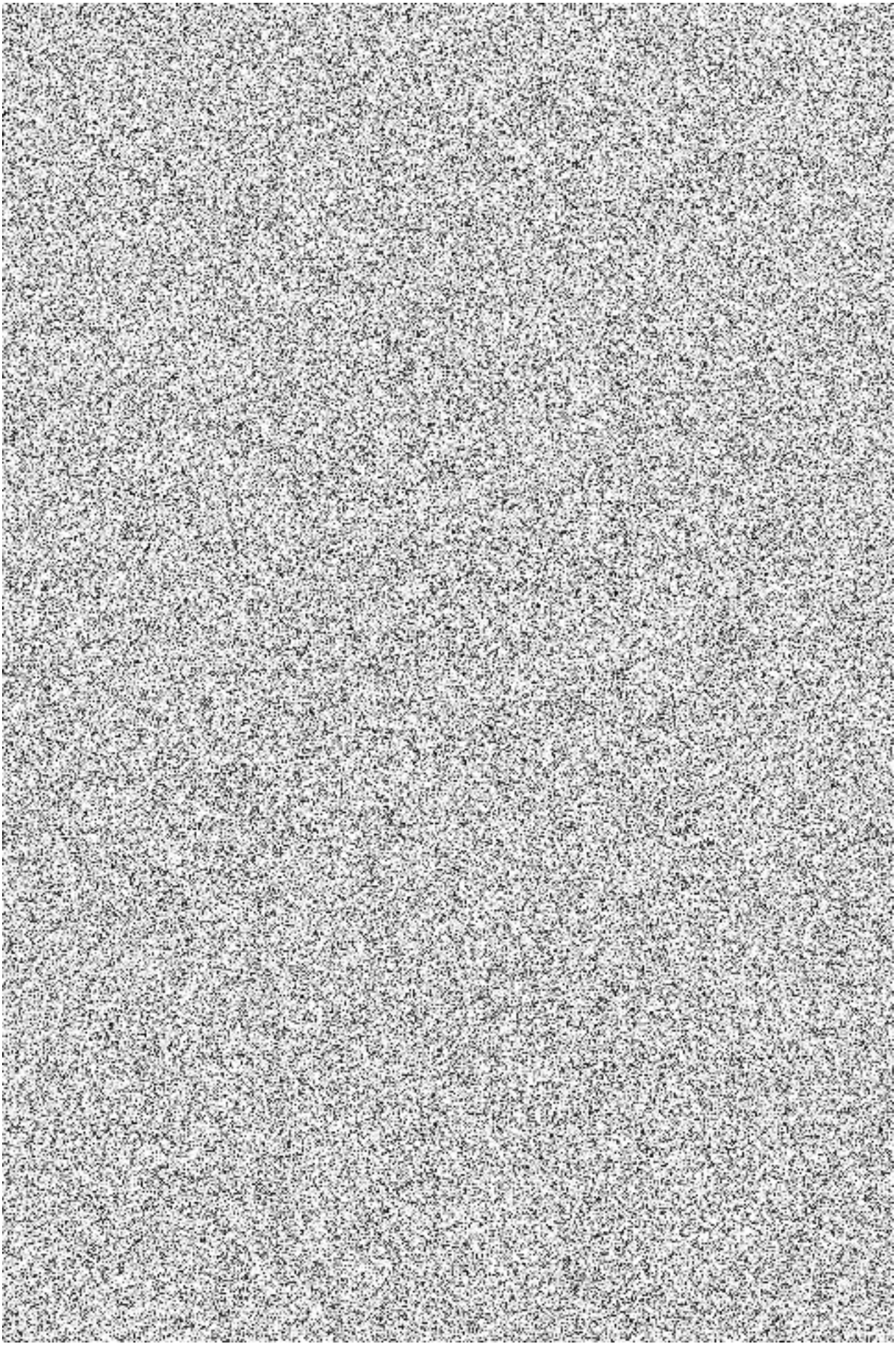


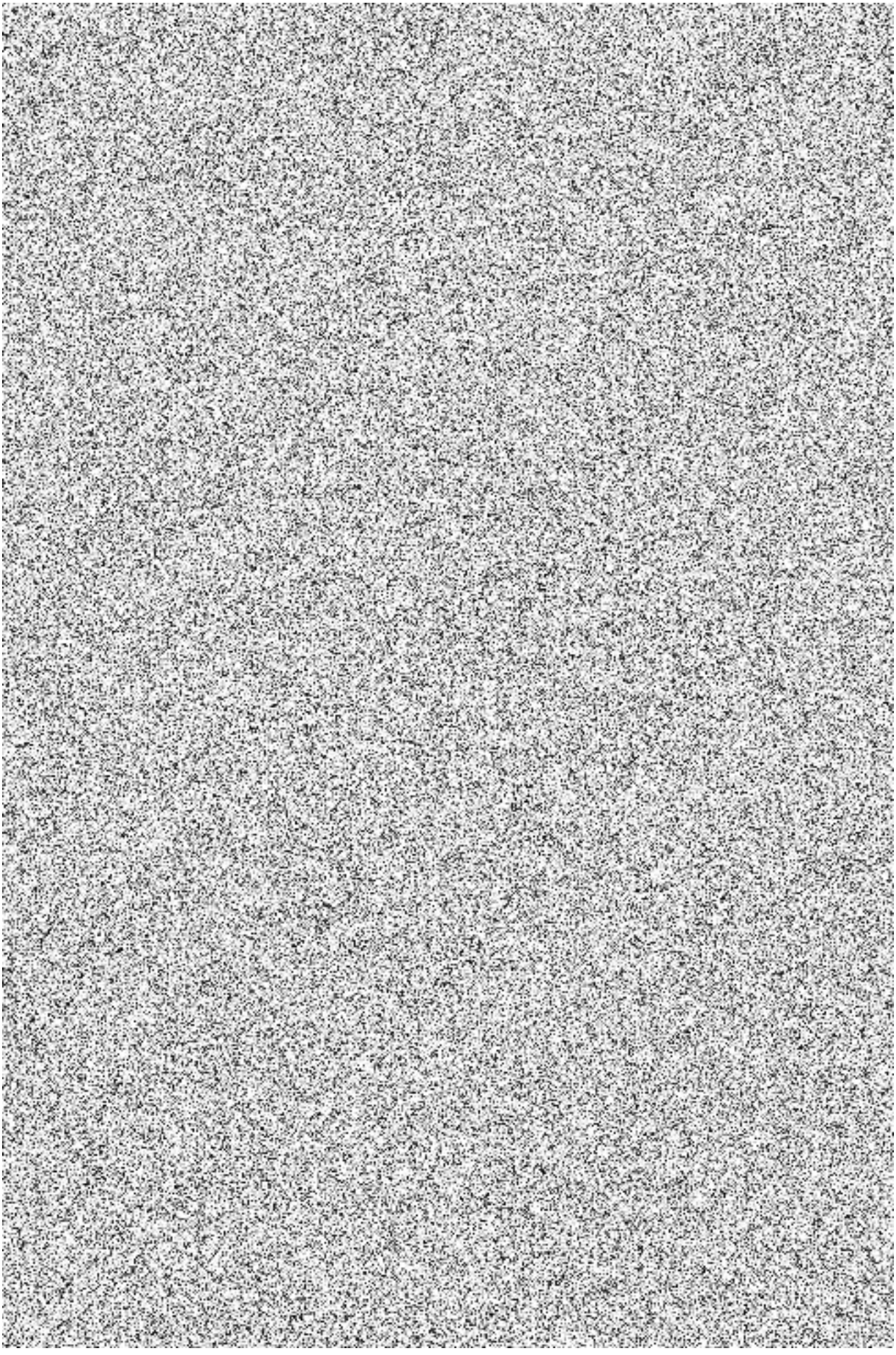


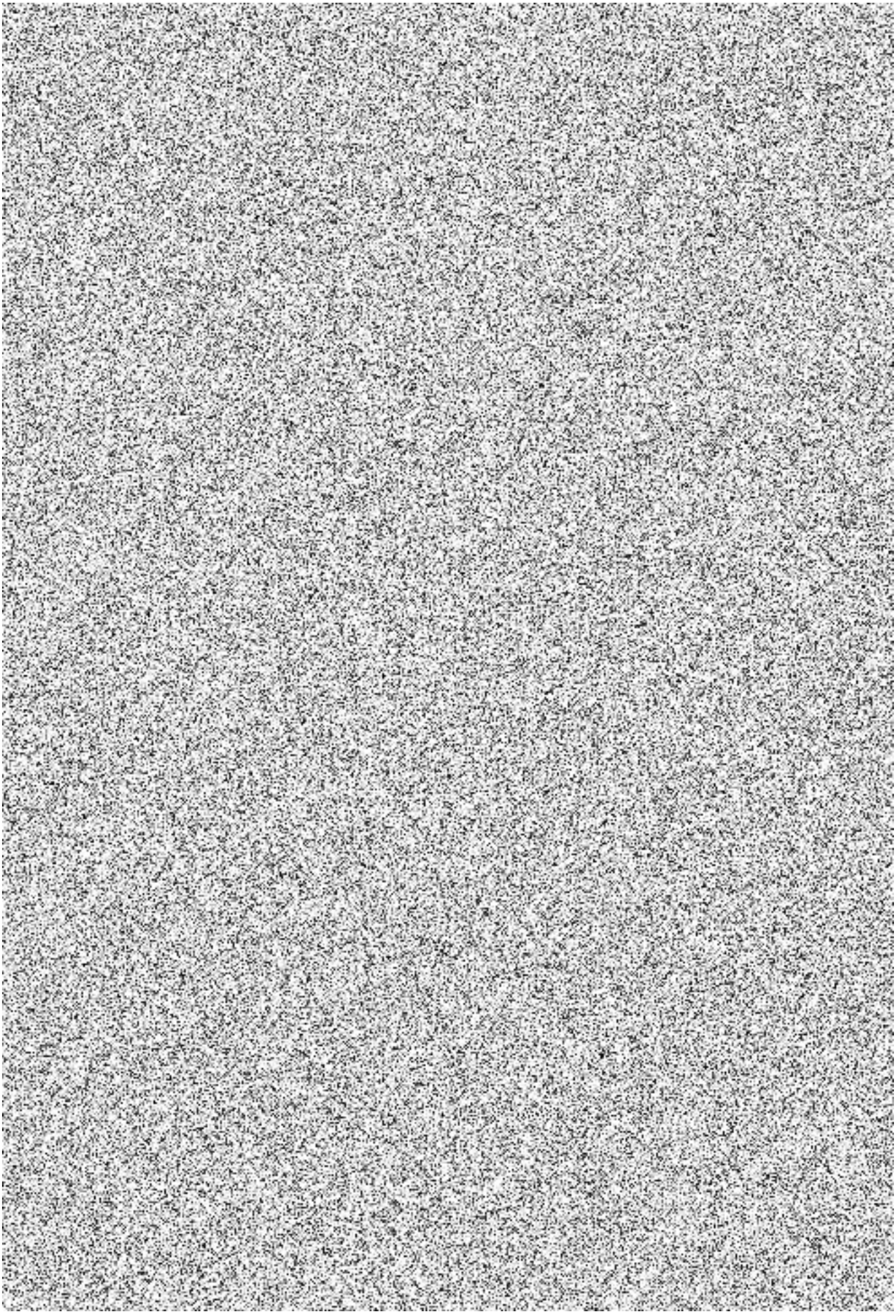


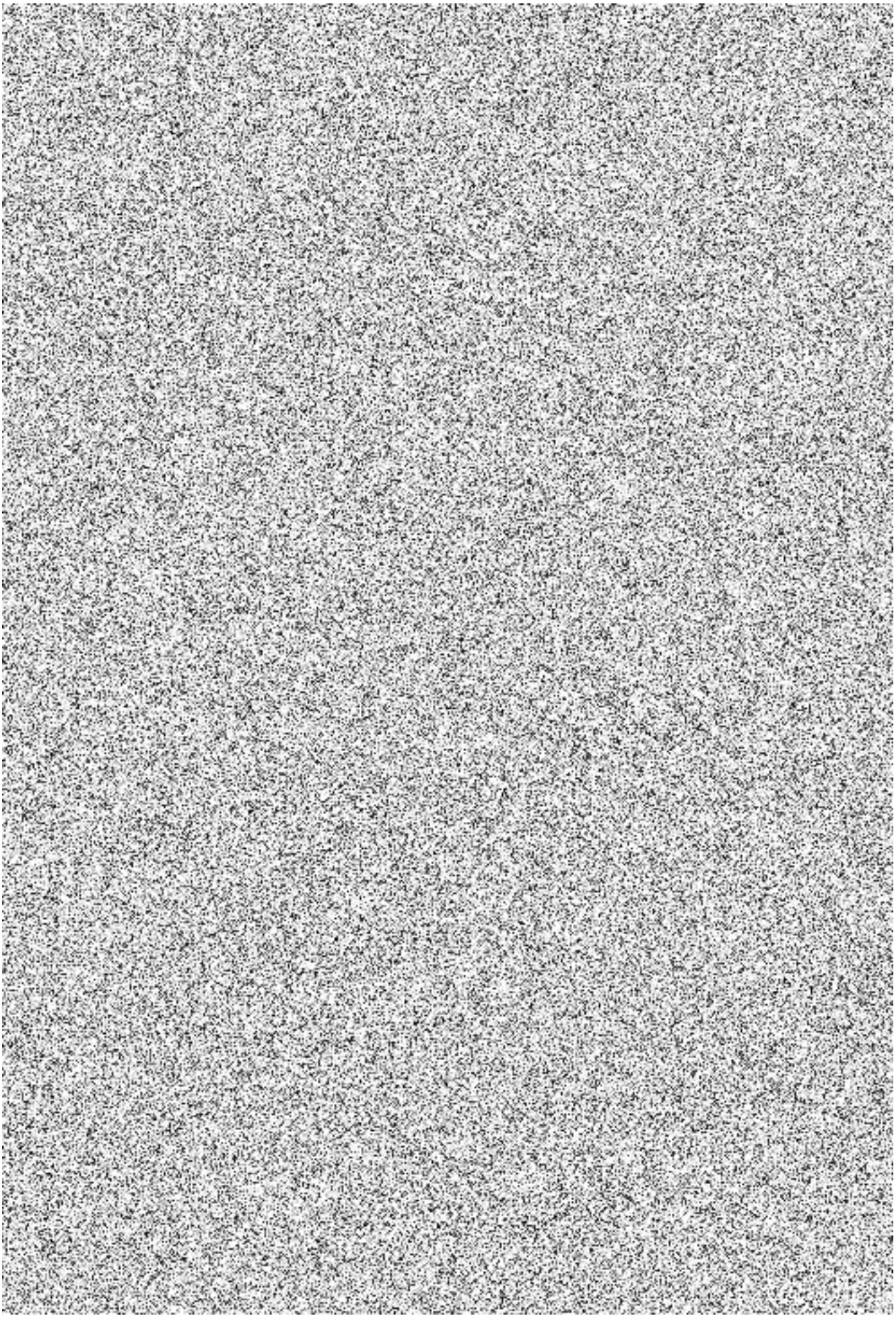


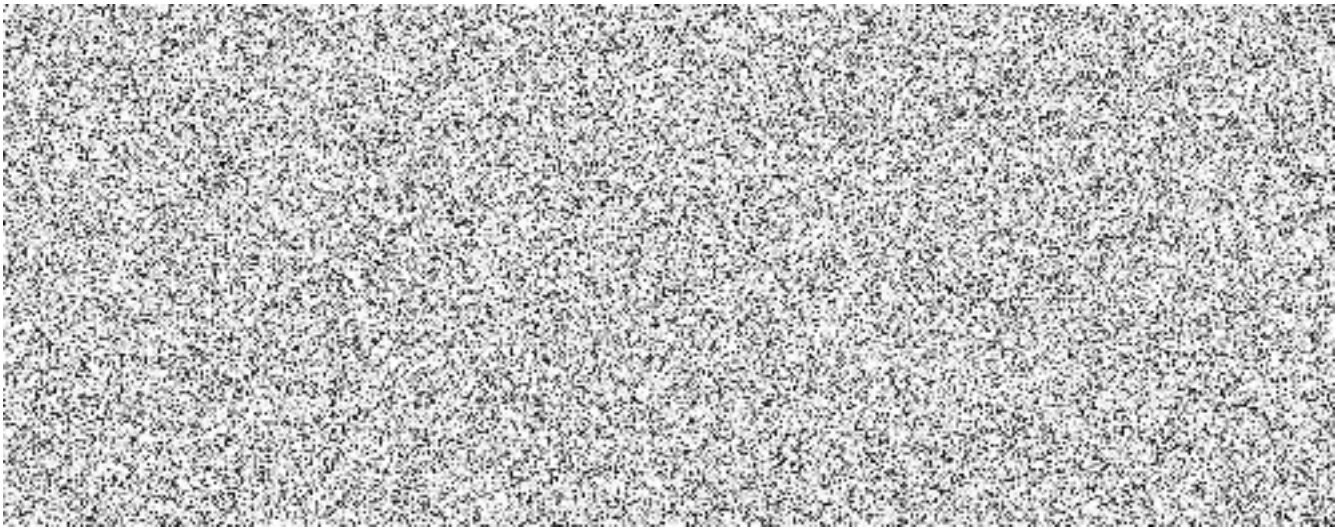


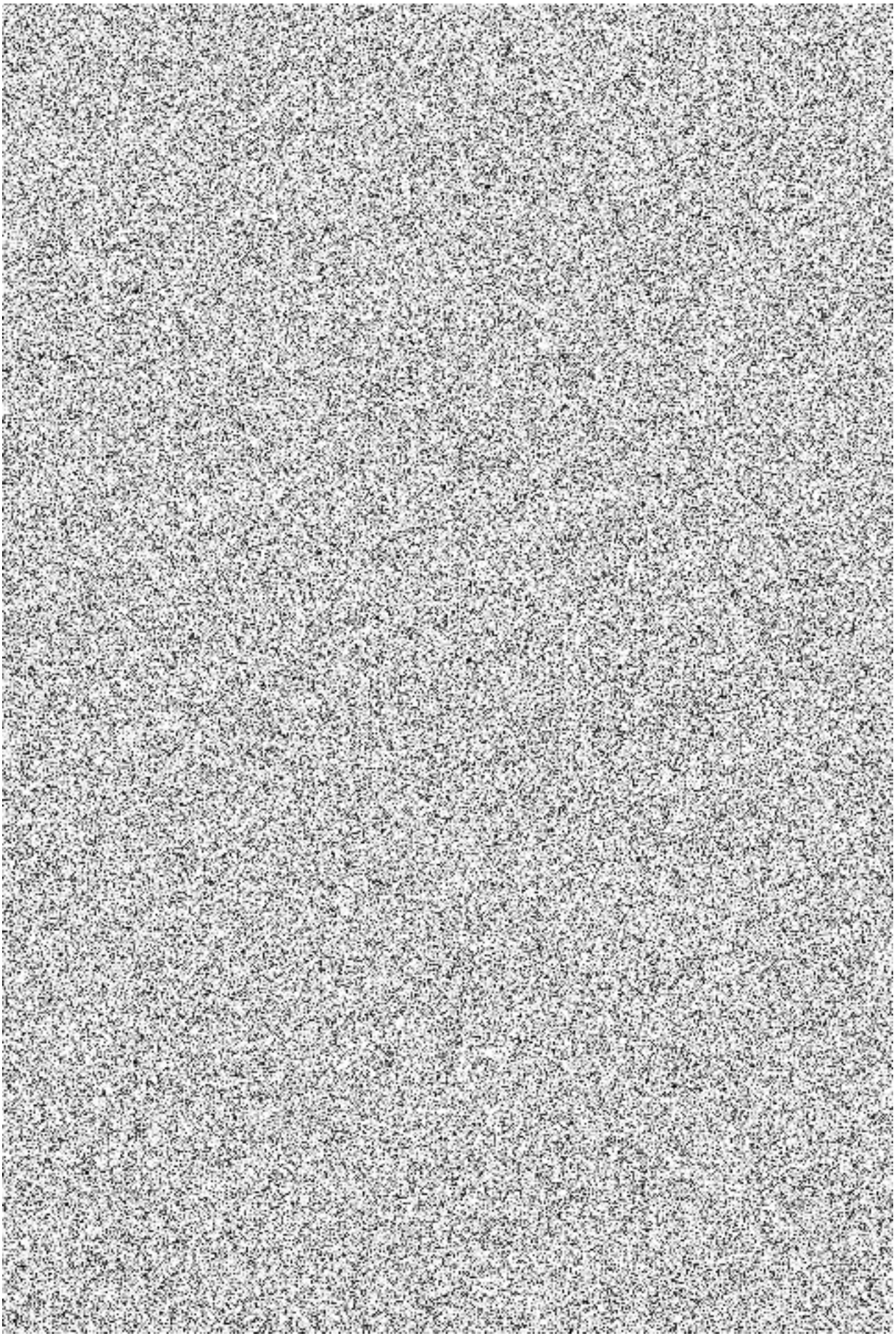


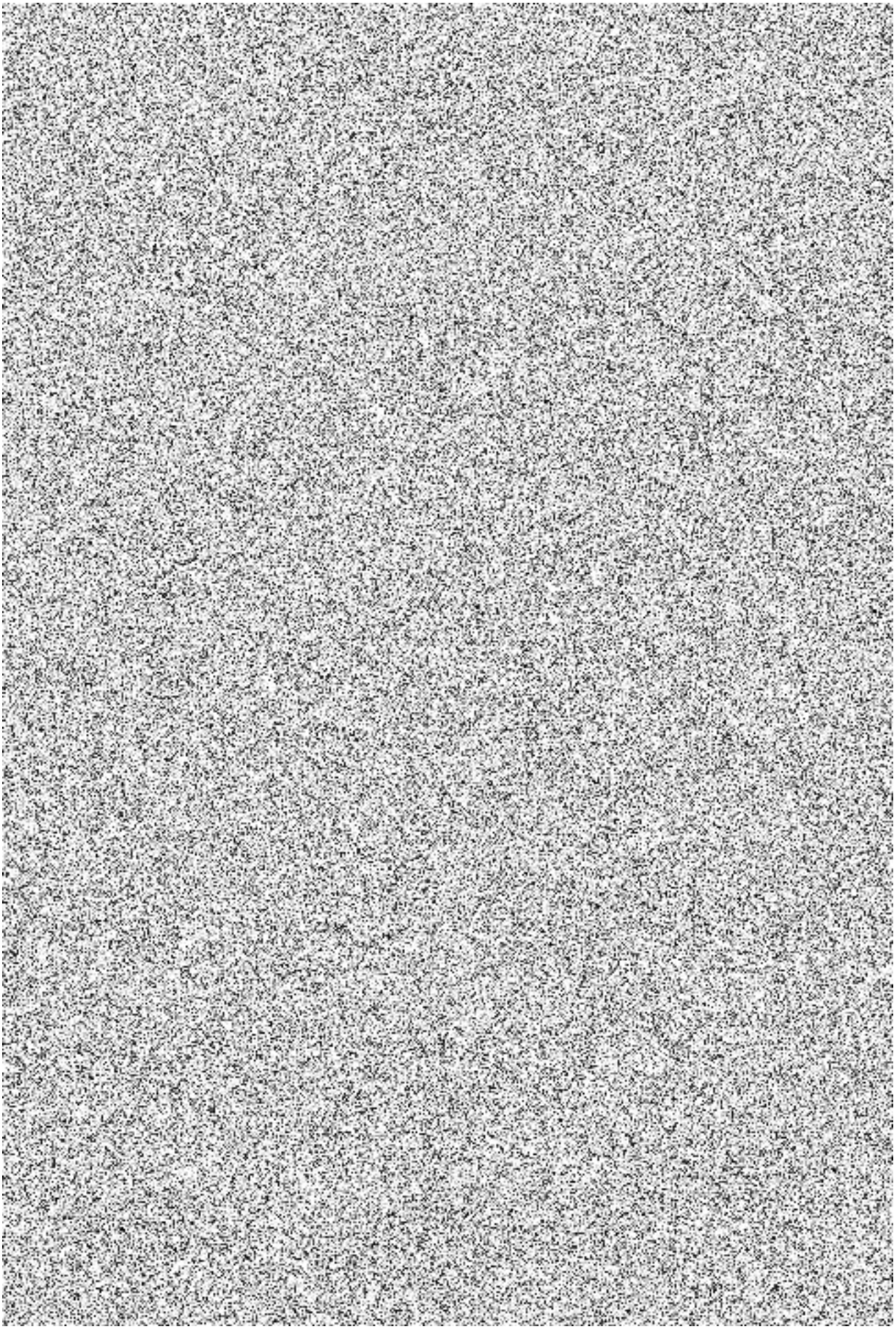


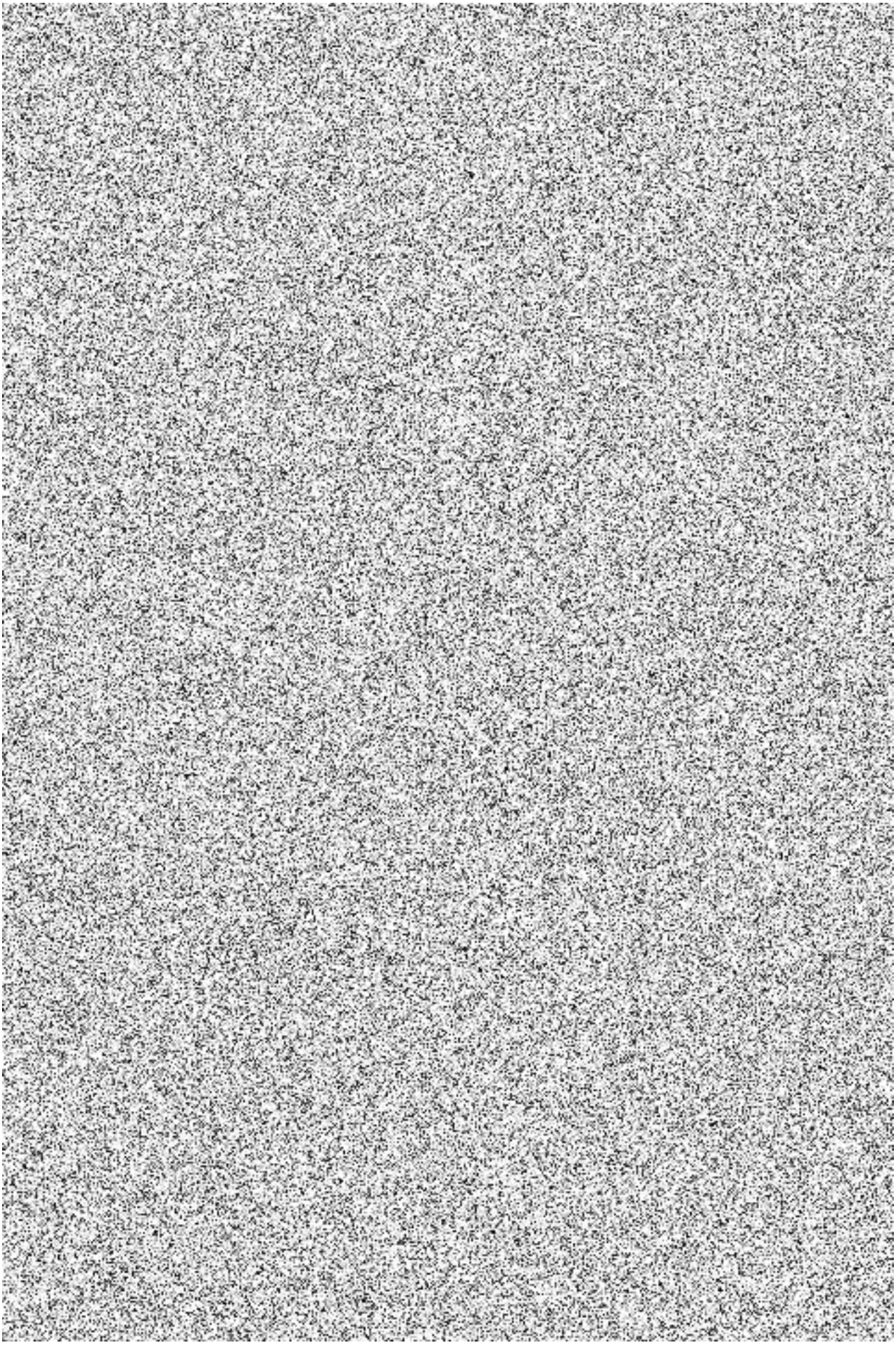


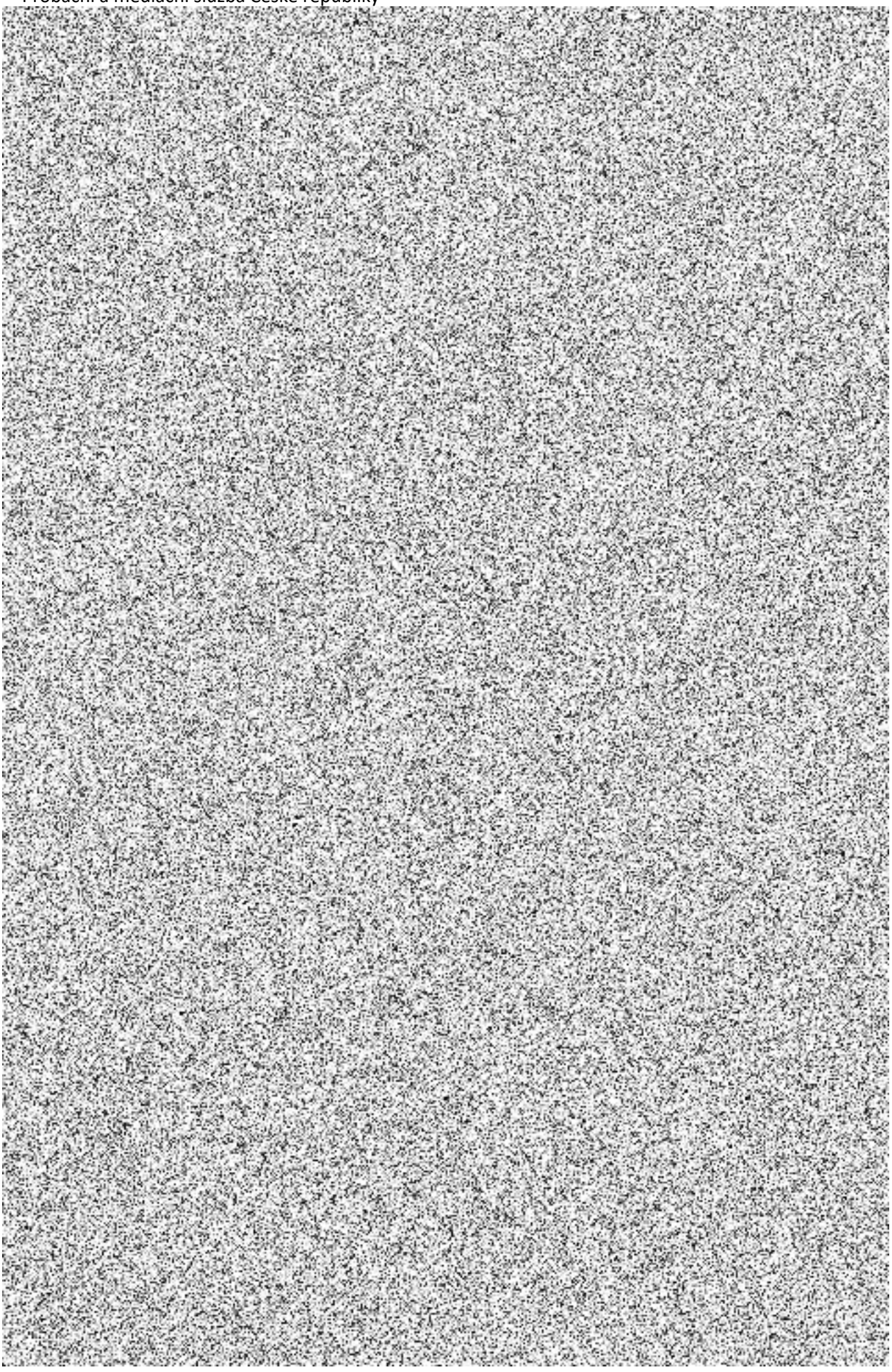


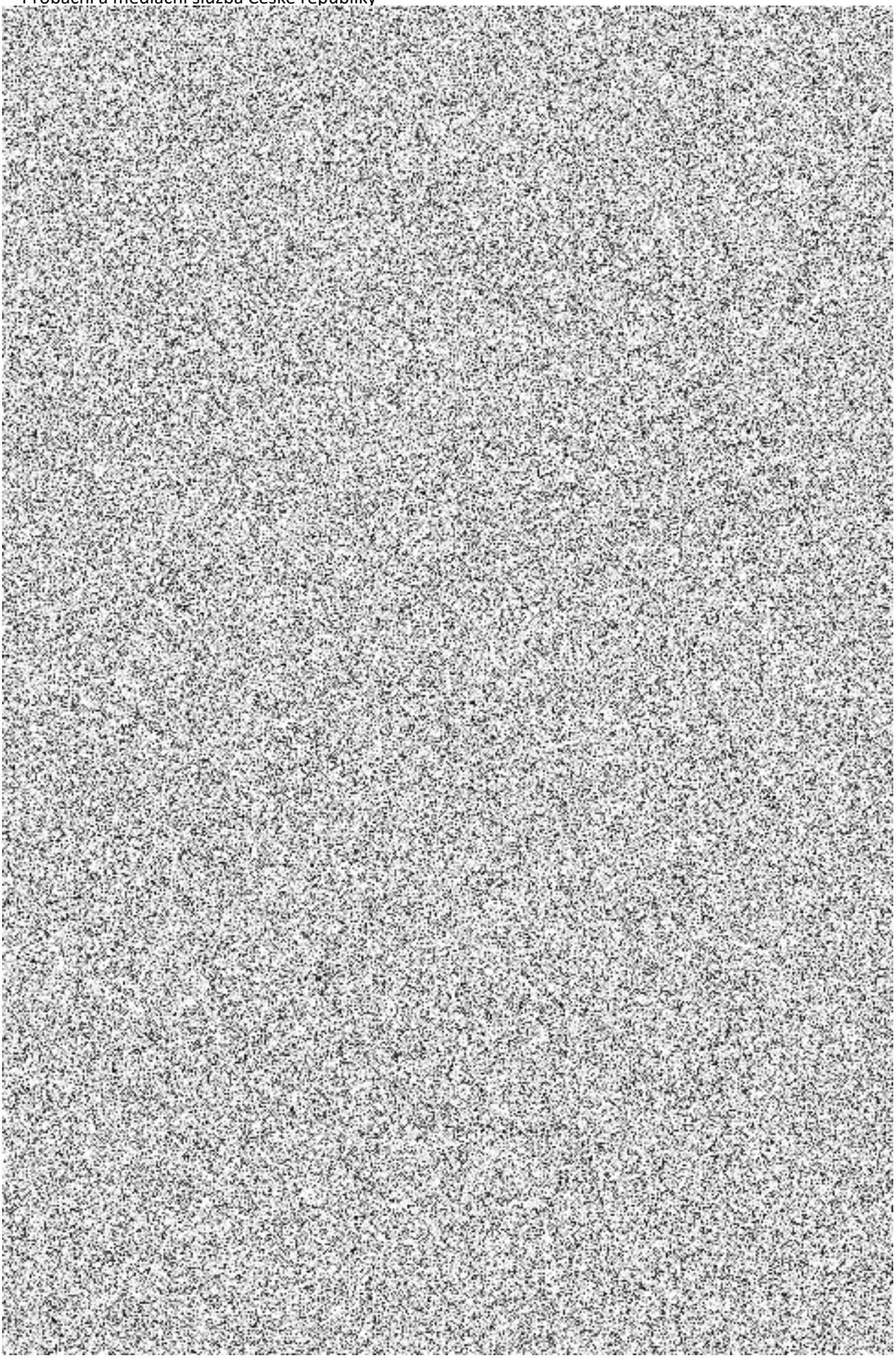


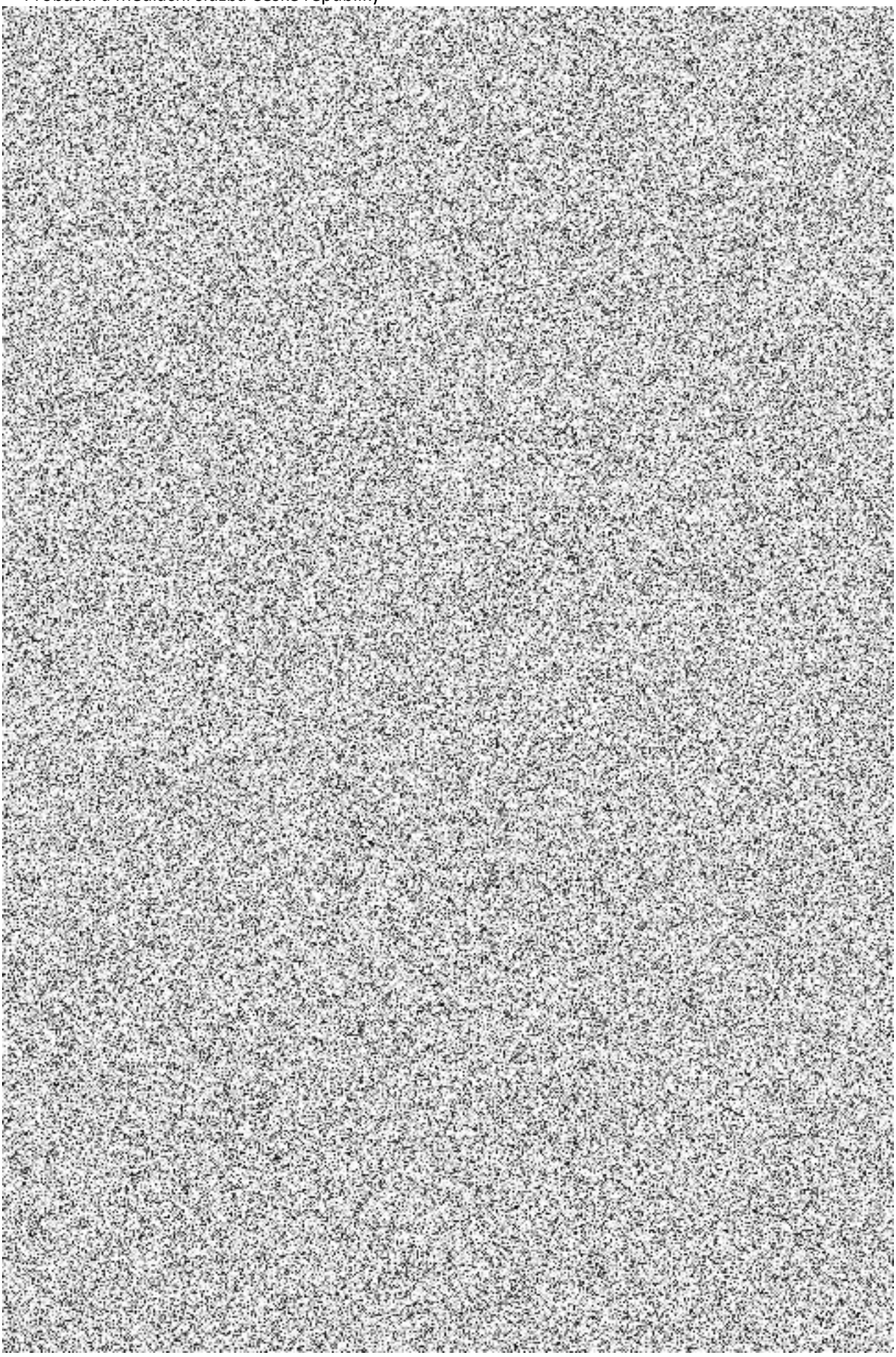


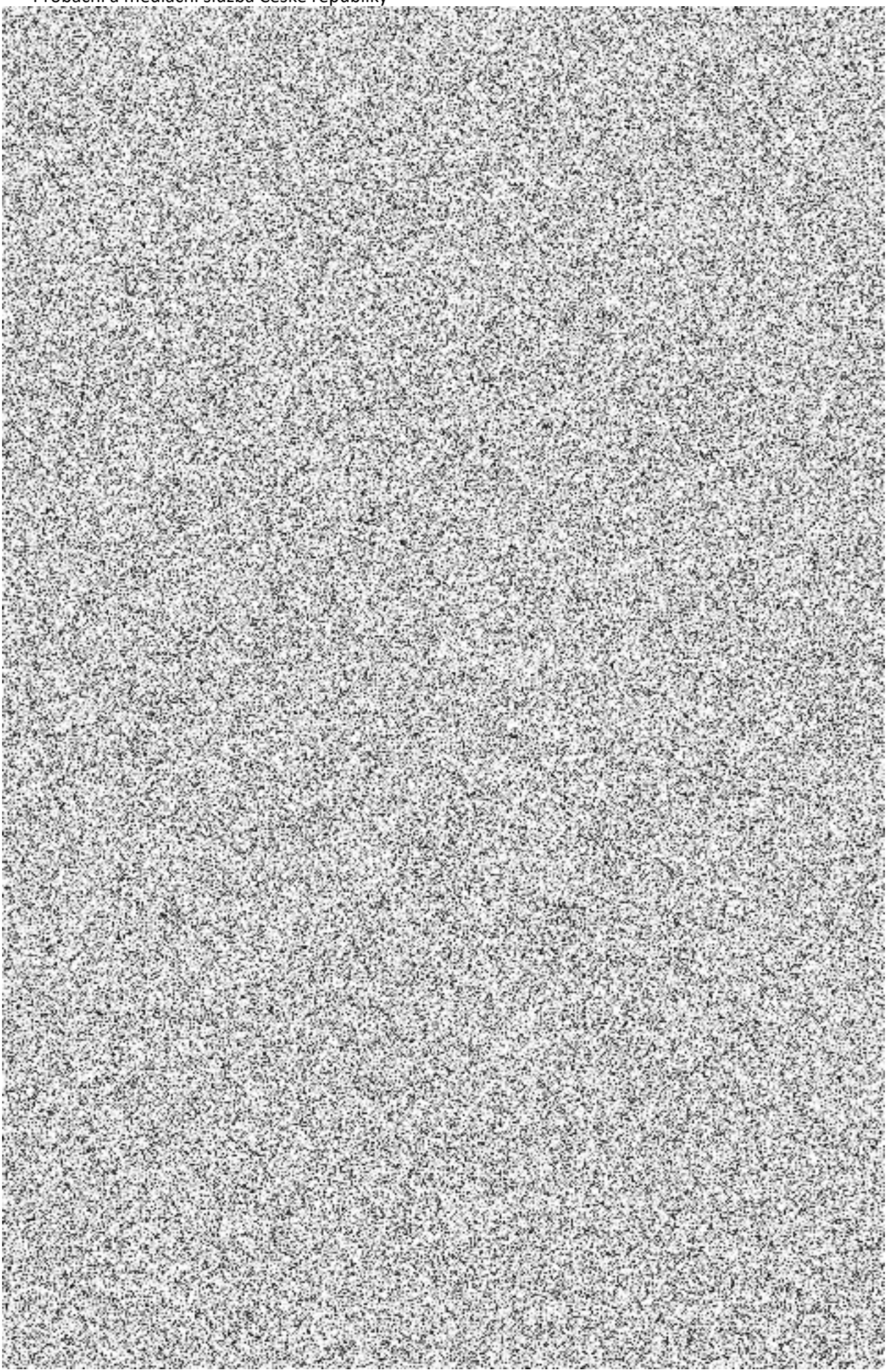


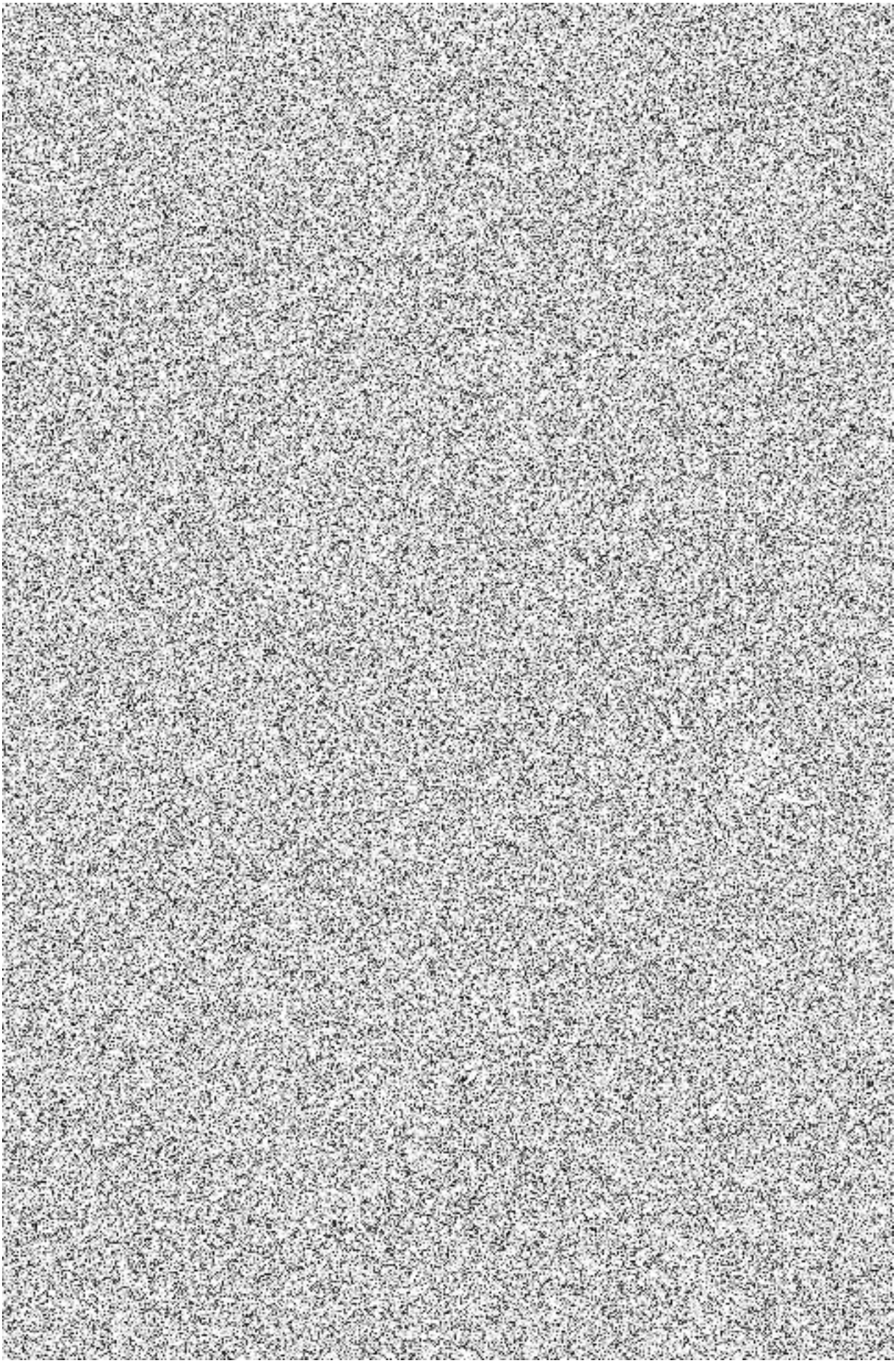


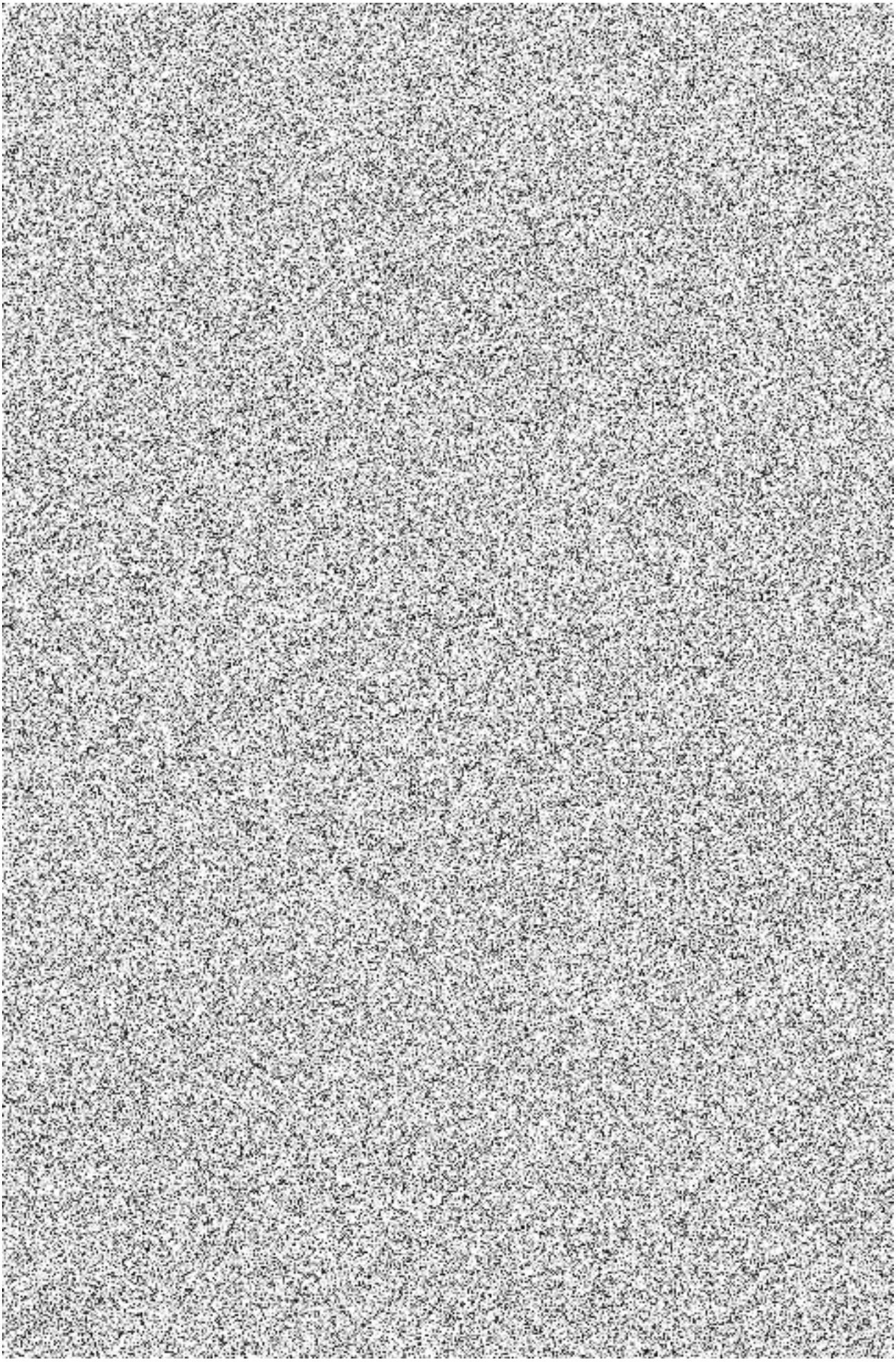


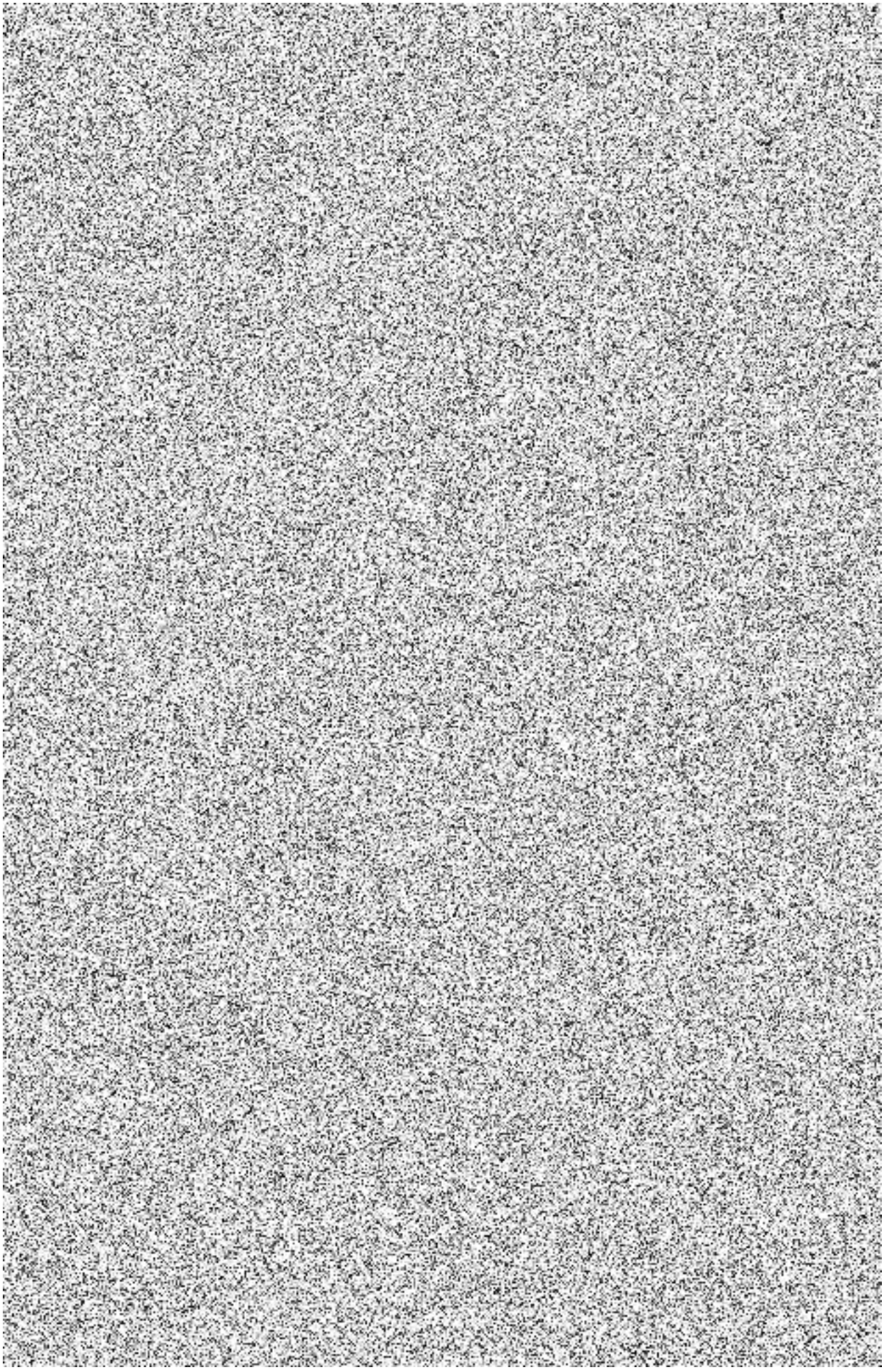


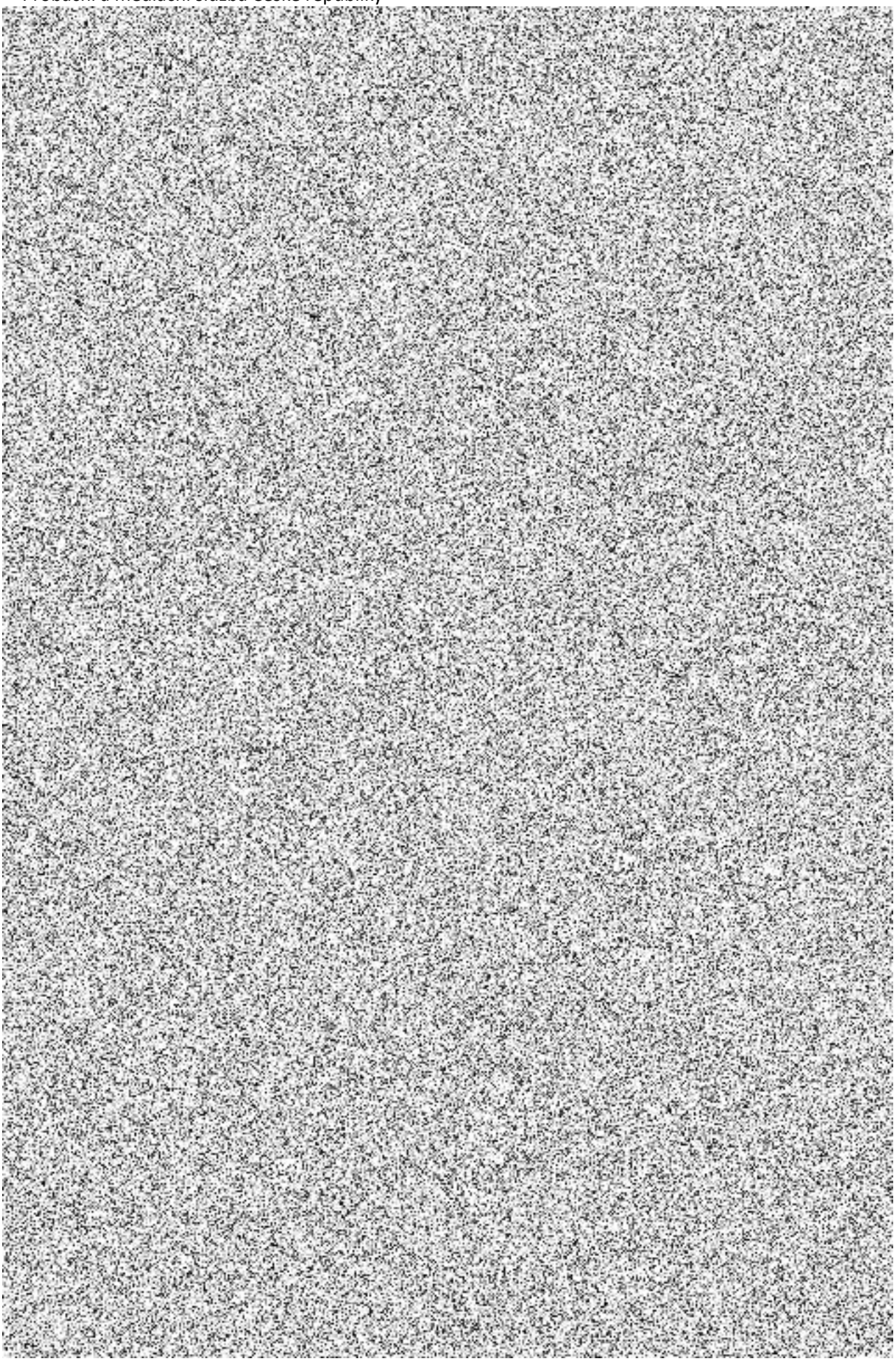


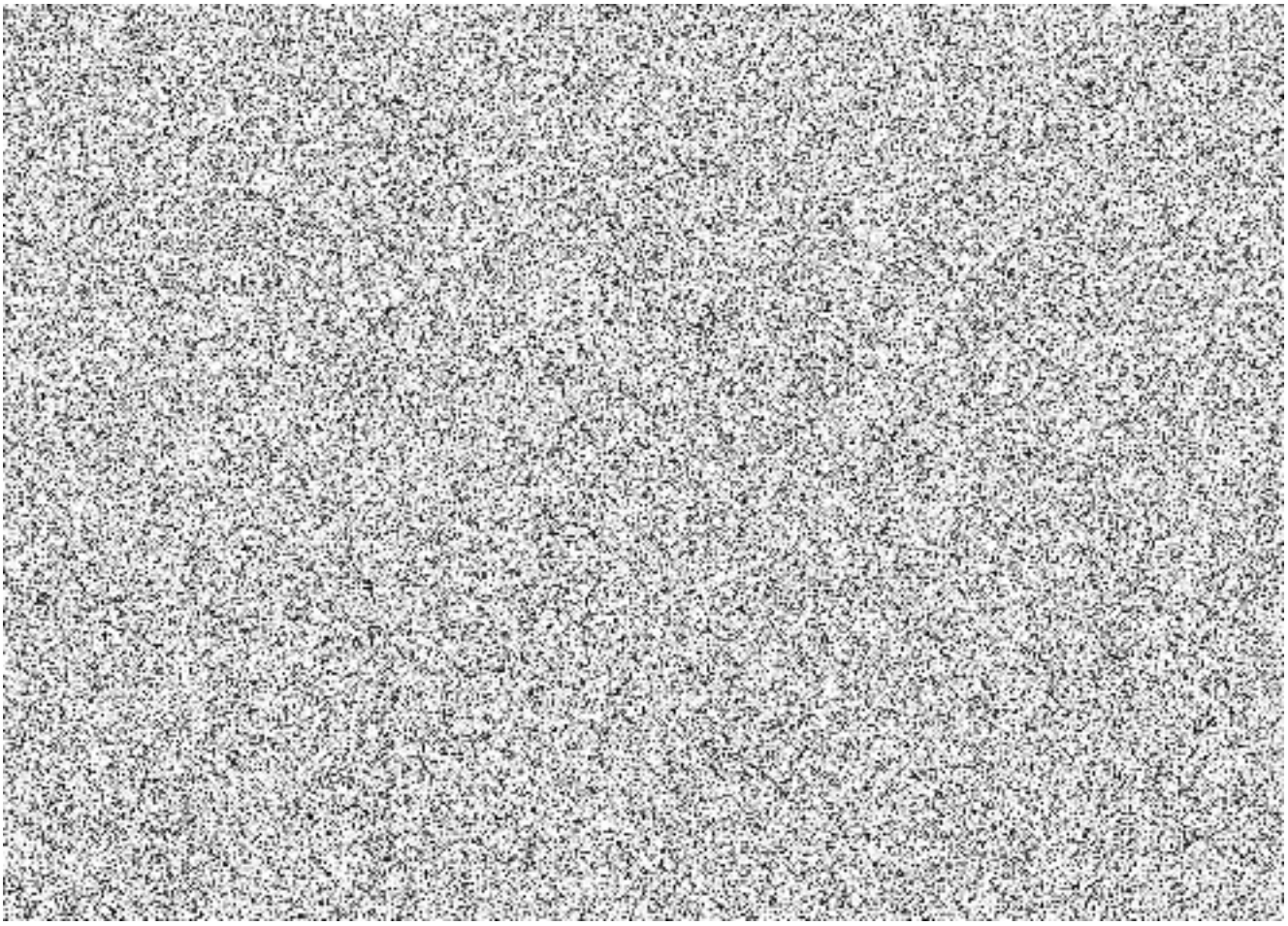






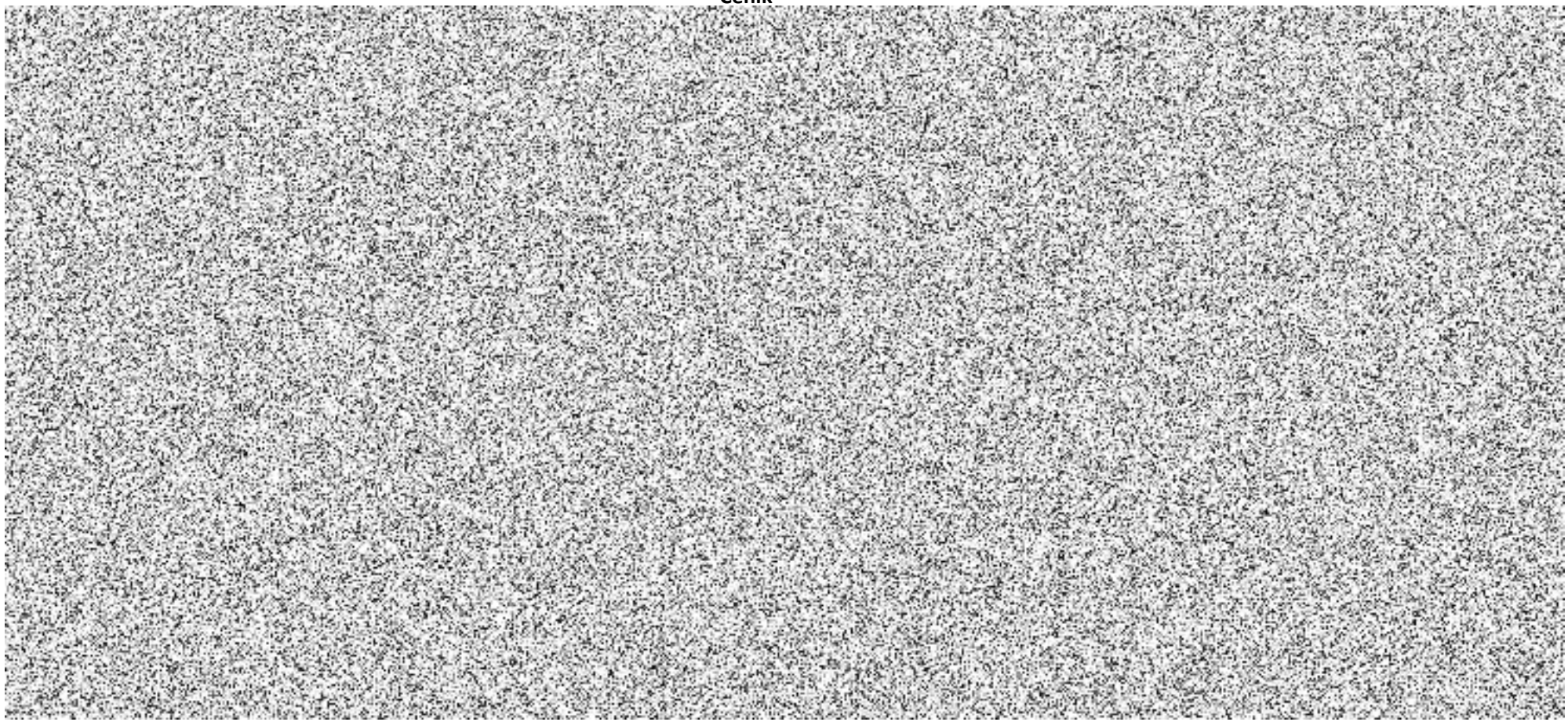






Příloha č. 2

Ceník



Příloha č. 3

Harmonogram

Klíčové termíny pro plnění Smlouvy, kdy T označuje okamžik účinnosti této Smlouvy.

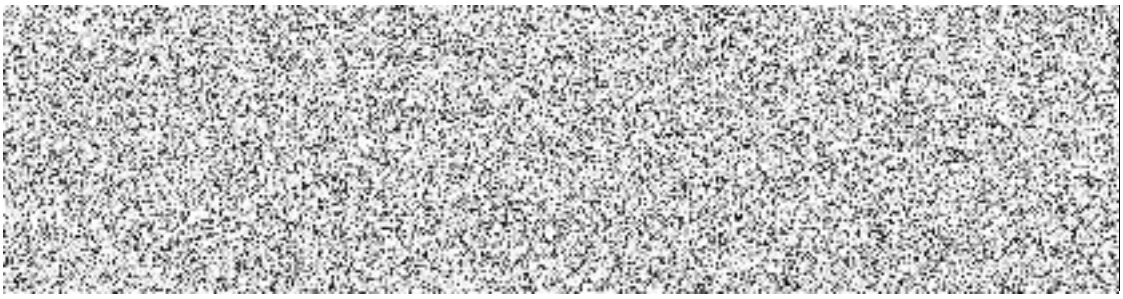
	Popis události	**Termín** **T – den nabytí účinnosti Smlouvy**
1	Akceptace Analýzy	T1 nejpozději T + 2 kalendářní měsíce
2	Akceptace Implementace	T2 nejpozději T + 5 kalendářních měsíců
3	Zahájení pilotního provozu EMS II	T3 T2 + jeden kalendářní den
4	Akceptace pilotního provozu EMS II	T4 T3 + 2 kalendářní měsíce
5	Zahájení ostrého provozu EMS II	T5 T4 + jeden kalendářní den

Příloha č. 4

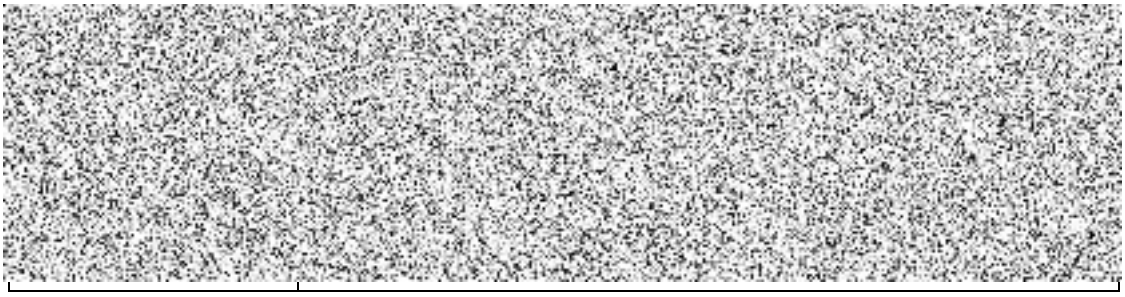
Oprávněné osoby

Za Objednatele:

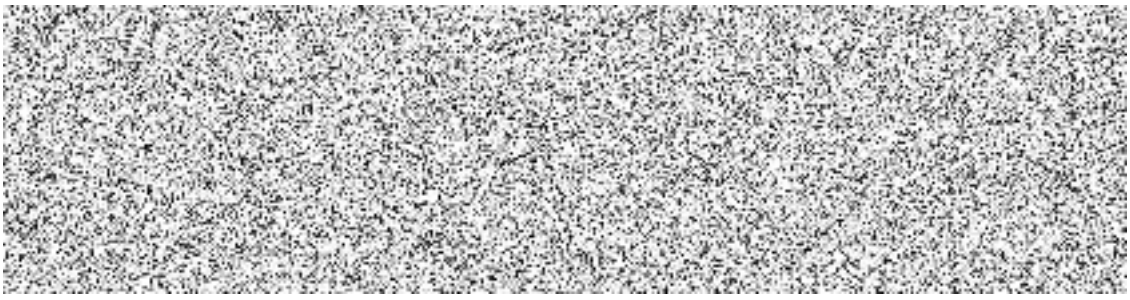
ve věcech smluvních:



ve věcech obchodních:

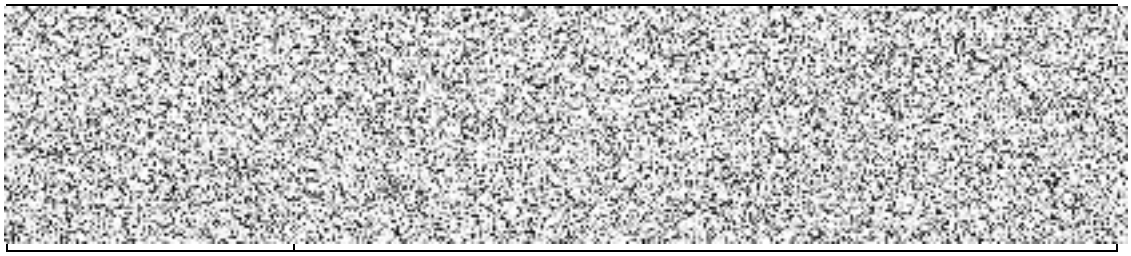


ve věcech technických:

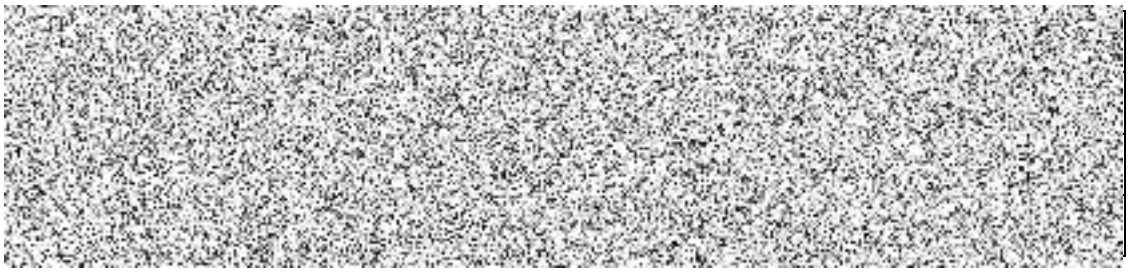


Za Dodavatele

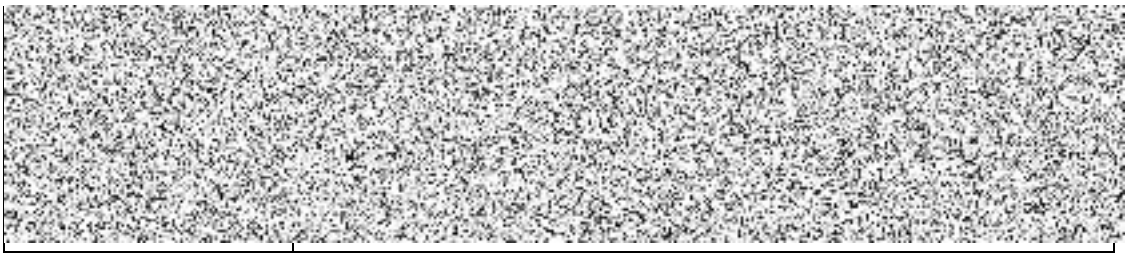
ve věcech smluvních:



ve věcech obchodních:



ve věcech technických:



Příloha č. 5

Realizační tým

Pozice člena týmu		Certifikace
Subject matter manager		certifikace Prince2 Practitioner Level
Projektový manažer		certifikace Prince2 Practitioner Level
Specialista architekt řešení		TOGAF 9 Foundation
Manažer kybernetické bezpečnosti		CISM a CISSP
Manažer podpory provozu		ITIL version 3

Příloha č. 6

Ochrana osobních údajů

1. ÚVODNÍ USTANOVENÍ

1.1. Vzhledem k tomu, že Dodavatel jako zpracovatel (dále pro účely této přílohy jako „**Zpracovatel**“) poskytuje Objednateli jako správci (dále pro účely této přílohy jako „**Správce**“) na základě Smlouvy služby, při nichž může docházet ke zpracování osobních údajů, uzavírají Smluvní strany toto ujednání o zpracování osobních údajů ve smyslu čl. 28 odst. 3 GDPR (dále jen „**Doložka**“).

1.2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků předpisů na ochranu osobních údajů (tyto zahrnují například zákon č. 110/2019 Sb., o zpracování osobních údajů, a GDPR; dále společně jen „**POOÚ**“), uzavřou bez zbytečného odkladu po výzvě kterékoli Smluvní strany písemný dodatek Smlouvy, v jehož rámci zohlední požadavky na úpravu Dodatku.

1.3. Pojmy použité v této Doložce, které v ní nejsou definovány, mají význam uvedený v GDPR.

1.4. Smluvní strany jsou povinny jednat v souladu s POOÚ a pravidly dopadajícími na jejich jednotlivé role v rámci zpracování osobních údajů, jak je blíže specifikováno dále v této Doložce.

2. PŘEDMĚT DOLOŽKY

2.1. Správce tímto pověřuje Zpracovatele zpracováním osobních údajů subjektů údajů poskytovaných Správcem v rámci plnění Smlouvy. Zpracovatel je povinen zpracovávat osobní údaje pro Správce na základě jeho pokynů a v rozsahu nezbytném k řádnému plnění povinností Zpracovatele vyplývajících ze Smlouvy a z Doložky.

3. PŘEDMĚT ZPRACOVÁNÍ, KATEGORIE SUBJEKTŮ ÚDAJŮ A TYP OSOBNÍCH ÚDAJŮ

3.1. Předmětem zpracování jsou osobní údaje subjektů údajů, zejména jméno a příjmení, informace o trestní řízení a trestu, adresa bydliště a kontaktní údaje, a případně další údaje poskytnuté Správcem či třetími stranami z pokynu Správce (dále jen „**Osobní údaje**“).

3.2. Subjekty údajů jsou Monitorované osoby.

4. POVAHA A ÚČEL ZPRACOVÁNÍ

4.1. Zpracovatel bude zpracovávat Osobní údaje automatizovaně s užitím statistických a analytických metod s přispěním výpočetní techniky. Příležitostně může docházet k ručnímu zpracování dat.

4.2. Účel zpracování Osobních údajů subjektů údajů je definován účelem plnění Smlouvy.

5. DOBA ZPRACOVÁNÍ

5.1. Zpracování Osobních údajů bude probíhat po dobu účinnosti Smlouvy. Povinnosti Zpracovatele týkající se ochrany Osobních údajů se Zpracovatel zavazuje plnit po celou dobu účinnosti Smlouvy, pokud ze Smlouvy nebo z Doložky nevyplývá, že mají trvat i po zániku její účinnosti.

6. PRÁVA A POVINNOSTI ZPRACOVATELE

6.1. Zpracovatel se zavazuje dodržovat všechny povinnosti, které vyplývají z POOÚ, jakož i z interních předpisů Správce a rozhodnutí či doporučení nebo stanovisek vydaných pro Správce příslušným orgánem státní správy, s nimiž byl seznámen, a to včetně rozhodnutí či stanovisek nebo doporučení vydaných v budoucnu.

6.2. Zpracovatel při zpracování Osobních údajů:

6.2.1. zpracovává Osobní údaje výlučně na základě doložených pokynů Správce; pro vyloučení pochybností, zpracování Osobních údajů v souladu s povinnostmi Zpracovatele dohodnutými v rámci Smlouvy a Doložky se považuje za prováděné v souladu s pokyny Správce;

6.2.2. řídí se instrukcemi Správce v otázkách předání Osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Evropské unie nebo členského státu, které se na Zpracovatele vztahuje; v takovém případě Zpracovatel Správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;

6.2.3. v případě, kdy je ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu provedena kontrola zpracování Osobních údajů Zpracovatelem či v případě zahájení správního řízení ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu ve vztahu ke zpracování Osobních údajů Zpracovatelem, oznámí tuto skutečnost okamžitě Správci a poskytne mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového řízení;

6.2.4. poskytne Správci součinnost při komunikaci s dozorovým orgánem a dle pokynů Správce bude spolupracovat při přípravě odpovědí dozorovému úřadu ohledně činností prováděných Zpracovatelem;

6.2.5. nezpracovává Osobní údaje získané za účelem plnění Smlouvy a Doložky pro své vlastní účely;

6.2.6. nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Správce;

6.2.7. při zohlednění povahy zpracování je Správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Správcovy povinnosti reagovat na žádosti o výkon práv subjektů údajů;

6.2.8. je Správci nápomocen při zajišťování souladu s povinnostmi Správce (i) zajistit úroveň zabezpečení zpracování, (ii) ohlašovat případy porušení zabezpečení Osobních údajů Úřadu pro ochranu osobních údajů a případně též subjektům údajů, (iii) posuzovat vliv na ochranu Osobních údajů (výstupem tohoto posouzení bude poskytnutí podkladových materiálů a vlastních odborných vyjádření) a (iv) realizovat předchozí konzultace s Úřadem pro ochranu osobních údajů, a to při zohlednění povahy zpracování a informací, jež má Zpracovatel k dispozici;

6.2.9. v souladu s rozhodnutím Správce všechny Osobní údaje buď vymaže, nebo vrátí Správci po ukončení poskytování plnění dle Smlouvy, a vymaže existující kopie, pokud právo Evropské unie nebo členského státu nepožaduje uložení daných Osobních údajů;

6.2.10. poskytuje Správci veškeré informace a dokumenty potřebné k doložení toho, že byly splněny povinnosti stanovené touto Doložkou a POOÚ;

6.2.11. není oprávněn Osobní údaje jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností dle Smlouvy nebo Doložky;

6.2.12. zajišťuje, aby se osoby oprávněné zpracovávat Osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

6.2.13. umožní Správci na vyžádání kontrolu dodržování povinností dle tohoto čl. 6.2 Smlouvy, zejména přístupy do prostor, v nichž jsou Osobní údaje uchovávány, předložení seznamu osob s přístupem k Osobním údajům či doložení, že veškeré osoby přistupující k Osobním údajům splňují požadavky Pověřené osoby, jak je tato definována níže; a

6.2.14. umožní Správci přístup do informačního systému užívaného pro zpracování Osobních údajů a k probíhajícím operacím zpracování.

6.3. Zpracovatel umožní Správci či jinému auditorovi, kterého Správce pověří, provést audit, včetně inspekcí, kontroly způsobu zpracování Osobních údajů a technických a organizačních opatření zavedených Zpracovatelem k ochraně Osobních údajů a k takovému auditu přispěje. Správce je povinen o záměru provést audit vyrozumět Zpracovatele nejméně s předstihem 3 pracovních dnů. Oznámení podle předchozí věty není potřeba v případě, kdy hrozí ohrožení Osobních údajů nebo již k takovému ohrožení již došlo. Každá ze Smluvních stran nese své vlastní náklady související s provedením auditu. Ustanovení předchozí věty neplatí v případě, že během auditu budou zjištěna závažná pochybení Zpracovatele a v takovém případě nese veškeré náklady na provedení auditu Zpracovatel.

6.4. V souvislosti se zpracováním Osobních údajů vede Zpracovatel v souladu s POOÚ záznamy o všech kategoriích činností zpracování prováděných pro Správce v písemné či elektronické formě, jež obsahují zejména:

6.4.1. jméno a kontaktní údaje Zpracovatele, Správce a případného zástupce Správce nebo Zpracovatele a pověřence pro ochranu osobních údajů;

6.4.2. kategorie zpracování prováděného pro Správce;

6.4.3. informace o případném předání Osobních údajů do třetí země nebo mezinárodní organizaci; a

6.4.4. popis technických a organizačních bezpečnostních opatření.

Zpracovatel se na základě písemné výzvy Správce zavazuje Správci vedené záznamy bez zbytečného odkladu zpřístupnit.

6.5. Zpracovatel zajišťuje, kontroluje a odpovídá za:

6.5.1. plnění pokynů pro zpracování Osobních údajů osobami, které mají bezprostřední přístup k Osobním údajům;

6.5.2. zabránění neoprávněným osobám přistupovat k Osobním údajům a k prostředkům pro jejich zpracování;

6.5.3. zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících Osobní údaje; a

6.5.4. opatření, která umožní určit a ověřit, komu byly Osobní údaje předány.

6.6. V případě, že je podle POOÚ vyžadováno jakékoli oznámení nebo jiný úkon vůči správnímu orgánu, upozorní Zpracovatel na tuto skutečnost Správce v dostatečném předstihu a v případě, že tím Správce Zpracovatele pověří a zmocní, zajistí provedení těchto úkonů.

6.7. Pokud Zpracovatel zjistí, že Správce porušuje povinnosti podle POOÚ, je povinen jej na to neprodleně upozornit.

6.8. Vznikne-li Správci v důsledku nesplnění povinnosti Zpracovatele dle POOÚ újma (škoda i nemajetková újma), zavazuje se Zpracovatel Správci tuto újmu v plném rozsahu nahradit. Újmou vzniklou Správci se pro účely tohoto ustanovení rozumí zejména (i) náhrada újmy (škody i

nemajetkové újmy) subjektům údajů ve smyslu POOÚ a (ii) pokuty uložené Úřadem pro ochranu osobních údajů či jiným správním úřadem.

6.9. Plnění povinností a součinnost Zpracovatele dle Doložky je součástí ceny za služby poskytované dle Smlouvy.

7. ZAPOJENÍ DALŠÍCH ZPRACOVATELŮ

7.1. V návaznosti na odst. 6.2.6 Doložky, Správce nesouhlasí se zapojením dalších zpracovatelů do zpracování Osobních údajů. Zpracovatel je povinen písemně oznámit Správce záměr zapojit do zpracování Osobních údajů dle tohoto článku dalšího zpracovatele včetně konkrétní identifikace tohoto dalšího zpracovatele a vyžádat si jeho souhlas.

7.2. Pokud Zpracovatel zapojí do zpracování Osobních údajů dalšího zpracovatele, musí se tento další zpracovatel smluvně zavázat k dodržování stejných povinností na ochranu Osobních údajů, jako jsou dohodnuty mezi Správcem a Zpracovatelem, a to zejména k zavedení vhodných technických a organizačních opatření.

8. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

8.1. Zpracovatel přijal a udržuje taková technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k Osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití Osobních údajů.

8.2. Zpracovatel je povinen zajistit, že přístup k Osobním údajům bude umožněn výlučně pověřeným osobám, které budou v pracovněprávním, příkazním či jiném obdobném poměru ke Zpracovateli, budou předem prokazatelně seznámeny s povahou Osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se zpřístupněním Osobních údajů a jejich zpracováním (dále jen „**Pověřené osoby**“). Splnění této povinnosti zajistí Zpracovatel vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání. Přístup k Osobním údajům bude Pověřeným osobám umožněn výlučně pro účely zpracování Osobních údajů v rozsahu a za účelem stanoveným v Doložce.

8.3. Zpracovatel dále vhodným způsobem zajistí, že Pověřené osoby budou zpracovávat Osobní údaje na základě smlouvy se Zpracovatelem a že budou zpracovávat Osobní údaje pouze za podmínek a v rozsahu Zpracovatelem stanoveném a odpovídajícím Doložce a právním předpisům, zejména zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací Pověřených osob.

8.4. Zpracovatel vyvine maximální možné úsilí k tomu, aby:

8.4.1. zajistil, aby Pověřené osoby měly přístup pouze k Osobním údajům odpovídajícím oprávnění Pověřených osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;

8.4.2. pořizoval elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly Osobní údaje zaznamenány nebo jinak zpracovány;

8.4.3. zabránil neoprávněnému přístupu k datovým nosičům.

8.5. Zpracovatel přijme zejména následující opatření k zajištění přiměřené úrovně zabezpečení:

8.5.1. víceúrovňový firewall;

8.5.2. antivirovou ochranu a kontrolu neoprávněných přístupů;

8.5.3. přístup k Osobním údajům mají pouze Pověřené osoby; a

8.5.4. servery s Osobními údaji jsou uzamčeny v datacentrech Zpracovatele.

8.6. Zpracovatel se dále zavazuje přijmout následující opatření, jsou-li s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob nezbytná k zajištění odpovídající úrovně zabezpečení:

8.6.1. pseudonymizace a šifrování Osobních údajů;

8.6.2. schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování – zavedená opatření a jejich korektní fungování budou pravidelně kontrolovány;

8.6.3. schopnost obnovit dostupnost Osobních údajů a přístup k nim včas a v případě fyzických či technických incidentů;

8.6.4. proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;

8.6.5. šifrovaný přenos dat.

8.7. Při zpracování Osobních údajů budou Osobní údaje uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat, jedná-li se o Osobní údaje v elektronické podobě. Zpracovatel nesmí ukládat Osobní údaje na veřejná uložiště bez předchozího svolení Správce.

8.8. Při zpracování Osobních údajů v jiné než elektronické podobě, budou Osobní údaje uchovány v místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně Pověřené osoby.

8.9. Zpracovatel se zavazuje na písemnou žádost Správce přijmout v přiměřené lhůtě stanovené Správcem další záruky za účelem technického a organizačního zabezpečení Osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k Osobním údajům.

8.10. V případě zjištění porušení záruk dle tohoto článku je Zpracovatel povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje, nejpozději však do 3 pracovních dnů poté, co je k tomu Správcem vyzván.

8.11. V případě, že se Zpracovatel po dobu účinnosti Doložky dozví o porušení zabezpečení Osobních údajů zpracovávaných Zpracovatelem, je povinen ohlásit Správci, že došlo k porušení zabezpečení Osobních údajů bez zbytečného odkladu, nejpozději do 24 hodin, poté, kdy se o něm dozvěděl. Následně bez zbytečného odkladu od okamžiku, kdy se Zpracovatel dozvěděl o případu porušení zabezpečení Osobních údajů, je Zpracovatel povinen Správci ohlásit popis povahy daného případu porušení zabezpečení Osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených osob a kategorií a přibližného množství dotčených záznamů Osobních údajů a popis pravděpodobných důsledků porušení zabezpečení Osobních údajů.

9. DOBA TRVÁNÍ A UKONČENÍ DOLOŽKY

9.1. Tato Doložka se uzavírá do skončení účinnosti Smlouvy.

9.2. V případě ukončení Doložky nejsou Zpracovatel, resp. jeho zaměstnanci, popř. pověřené třetí osoby, které přišly do styku s Osobními údaji, zbaveni mlčenlivosti. Povinnost mlčenlivosti u nich v takovémto případě trvá i po ukončení účinnosti Doložky, bez ohledu na trvání poměru uvedených osob k Zpracovateli.

9.3. V případě ukončení Doložky je Zpracovatel povinen ukončit jakékoli zpracování Osobních údajů a nejpozději do 30 dnů od ukončení účinnosti Doložky předat Správci protokolárně veškeré hmotné nosiče obsahující Osobní údaje a smazat veškeré Osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li Zpracovatel od Správce písemně jiné pokyny, pokud právo Evropské unie nebo členského státu nepožaduje uložení daných Osobních údajů.

Příloha č. 7

Kybernetická bezpečnost

1. OBECNÁ USTANOVENÍ

1.1 Tato příloha č. 7 (dále jen „**Příloha**“) tvoří nedílnou součást Smlouvy o dodání elektronického monitorovacího systému a poskytování dalších služeb (dále jen „**Smlouva**“).

1.2 Není-li dále stanoveno jinak nebo nevyplývá-li jinak z kontextu, mají pojmy počínající velkým písmenem v této Příloze shodný význam, jaký mají ve Smlouvě.

2. ROZSAH ZAPOJENÍ DODAVATELE A JEHO PODDODAVATELÉ

2.1 Rozsah zapojení Dodavatele na rozvoji a provozu primárních a podpůrných aktiv dle VKB je určen předmětem Smlouvy. Rozsah zapojení Dodavatele na zajištění bezpečnosti těchto aktiv je určen zejména touto Přílohou a Pravidly pro dodavatele a bezpečnostními politikami, jak jsou definována v odst. 3.1 Přílohy.

2.2 Dodavatel je oprávněn využít k plnění dle Smlouvy poddodavatele jen v případě, že to Smlouva výslovně připouští, a to za podmínek v ní uvedených. Dodavatel může ke schválení navrhnout nebo do plnění Smlouvy zapojit pouze takové poddodavatele, kteří nejsou v rozporu s požadavky Objednatele na Dodavatele, a kteří s ohledem na znalost informačních systémů Objednatele Dodavatelem, představují totožná a/nebo nižší rizika/zbytková rizika bezpečnosti informací, jako Dodavatel, nebo taková rizika zvyšují pouze nepatrným způsobem. Dodavatel je povinen zavázat poddodavatele k plnění shodných povinností, které plní vůči Objednateli dle této Přílohy a soustavně (případně pravidelně dle povahy) dohlížet na plnění této Přílohy poddodavatelem.

2.3 Dodavatel se zavazuje, že pravidla dle této Přílohy budou dodržovat i pracovníci Dodavatele, poddodavatelé Dodavatele a jejich pracovníci. Za porušení pravidel dle této Přílohy poddodavatelem odpovídá Dodavatel Objednateli tak, jako by je porušil sám.

2.4 Objednatel je oprávněn provést školení pravidel dle této Přílohy a školení Pravidel pro dodavatele a bezpečnostních politik pro pracovníky Dodavatele a jeho poddodavatelů, kteří mají přístup k aktivům Objednatele. Objednatel oznámí Dodavateli termín konání školení alespoň 14 pracovních dnů předem a určí pracovníky Dodavatele, kteří jsou povinni se školení zúčastnit. Objednatel současně zvolí formu a technické prostředky, prostřednictvím kterých bude školení probíhat. Školení ze strany Objednatele nezbavuje Dodavatele povinnosti provádět vlastní školení svých pracovníků a odpovědnosti za zajištění dostatečné znalosti pravidel dle této Přílohy a Pravidel pro dodavatele a bezpečnostních politik ze strany těchto pracovníků.

3. PRAVIDLA PRO DODAVATELE A BEZPEČNOSTNÍ POKYNY

3.1 Objednatel seznámil Dodavatele před podpisem Smlouvy s pravidly pro dodavatele a bezpečnostními politikami Objednatele, které zohledňují požadavky systému řízení bezpečnosti informací Objednatele, a které tvoří Přílohu č. 10 Smlouvy (dále jen „**Pravidla pro dodavatele a bezpečnostní politiky**“).

3.2 Dodavatel se s Pravidly pro dodavatele a bezpečnostními politikami seznámil před podpisem Smlouvy, což potvrzuje uzavřením Smlouvy, a zavazuje se dodržovat je, zejména s nimi seznámit pracovníky Dodavatele podílející se na poskytování plnění dle Smlouvy a písemně pracovníky Dodavatele zavázat k dodržování Pravidel pro dodavatele a bezpečnostních politik, a nejpozději před započetím poskytování plnění dle Smlouvy v souladu s § 8 odst. 1 písm. d) VKB Objednateli protokolárně potvrdit seznámení pracovníků a poddodavatelů s Pravidly pro dodavatele a bezpečnostní politikou.

3.3 Dodavatel se zavazuje zajistit, že k dodržování Pravidel pro dodavatele a bezpečnostních politik budou zavázáni také poddodavatelé Dodavatele a jejich pracovníci. Za porušení Pravidel pro dodavatele a bezpečnostních politik poddodavatelem odpovídá Dodavatel Objednateli tak, jako by je porušil sám.

3.4 V případě změny Pravidel pro dodavatele a bezpečnostních politik se Objednatel zavazuje aktuální znění bez zbytečného odkladu od provedení změny předat Dodavateli. Objednatel zašle Dodavateli aktuální znění způsobem pro doručování dle Smlouvy nebo do datové schránky. Dodavatel se zavazuje v přiměřené lhůtě a ne později, než 10 pracovních dnů od předání Pravidel pro dodavatele a bezpečnostních politik protokolárně Objednateli potvrdit, že se s aktuálním zněním Pravidel pro dodavatele a bezpečnostních politik seznámil, že se je zavazuje dodržovat, že s nimi seznámil pracovníky a poddodavatele Dodavatele podílející se na poskytování plnění dle Smlouvy a písemně pracovníky a poddodavatele Dodavatele zavázal k dodržování aktuálního znění Pravidel pro dodavatele a bezpečnostních politik a že zajistil, aby k dodržování Pravidel pro dodavatele a bezpečnostních politik byli zavázáni také pracovníci poddodavatelů Dodavatele. Současně, pokud aktuální znění Pravidel pro dodavatele a bezpečnostních politik ukládá Dodavateli přijetí nových bezpečnostních opatření, stanoví Objednatel, po konzultaci s Dodavatelem, termín pro jejich zavedení a implementaci.

4. POVINNOSTI PROVOZOVATELE

4.1 Dodavatel bere na vědomí, že nad rámec povinností stanovených touto Přílohou a Pravidly pro dodavatele a bezpečnostními politikami je jakožto provozovatel dle § 2 písm. g) ZKB povinen:

4.1.1 oznámit své kontaktní údaje příslušnému orgánu v souladu s § 16 ZKB;

4.1.2 zavádět bezpečnostní opatření dle potřeb Objednatele v souladu s § 4 ZKB;

4.1.3 hlásit kybernetické bezpečnostní incidenty v souladu s § 8 ZKB;

4.1.4 provádět opatření v souladu s § 11 ZKB (pokud dopadají do aktiv Objednatele pak v součinnosti s Objednatelem v nezbytném rozsahu k naplnění účelu opatření); a

4.1.5 předložit Objednateli výsledky auditu kybernetické bezpečnosti, pokud je proveden, v souladu s § 16 odst. 5 VKB.

5. DATA, JEJICH VYUŽITÍ A LIKVIDACE

5.1 Pokud v rámci poskytování plnění dle Smlouvy bude mít Dodavatel ve své dispozici data jemu předaná Objednatelem či jiným způsobem získaná nebo vytvořená při

plnění Smlouvy (dále jen „**Data**“), je oprávněn je při poskytování plnění dle Smlouvy užívat pouze v rozsahu a za podmínek dle Smlouvy.

5.2 Pokud Smlouva neobsahuje ujednání o užití Dat, pak je Dodavatel je oprávněn užít pouze v rozsahu nezbytném ke splnění Smlouvy, pouze v souladu se Smlouvou, touto Přílohou, zejm. odst. 5.2 až 5.5, ve Smlouvě vymezenými účely a v souladu s příslušnými právními předpisy, tj. zejména ZKB a VKB a pouze po dobu trvání Smlouvy (příp. povinnosti předat Data Objednateli).

5.3 Dodavatel se zavazuje zachovávat mlčenlivost a důvěrnost Dat a zavazuje se, že tato Data nebudou Dodavatelem nebo vinou Dodavatele zneužita, využita nebo poskytnuta třetím osobám. Současně Dodavatel omezí přístup k Datům pouze na nezbytný okruh osob s ohledem na plnění Smlouvy tak, aby byla efektivně chráněna důvěrnost, dostupnost a integrita Dat při zohlednění klasifikace Dat Objednatele.

5.4 Dodavatel se zavazuje na základě výzvy Objednatele bez zbytečného odkladu předat bezpečným způsobem, ve strojově čitelné podobě a ve formátu určeným v Příloze č. 1 Smlouvy zaručujícím kompatibilitu v procesu migrace jakákoli Data v dispoziční sféře Dodavatele. Dodavatel se k výzvě Objednatele zavazuje poskytnout nezbytnou součinnost, přičemž si Smluvní strany mohou písemně dohodnout jiný způsob předání Dat. Dodavatel je povinen i bez výzvy Objednatele předat Objednateli Data do 7 dnů po skončení účinnosti Smlouvy.

5.5 Dodavatel se zavazuje při ukončení účinnosti Smlouvy, případně na písemnou žádost Objednatele, bez zbytečného odkladu po předání Dat, nejpozději však do 14 dnů, zlikvidovat Data v souladu s Pravidly dodavatele a bezpečnostními politikami za podpůrného užití přílohy č. 4 VKB, to vše za možného dozoru zástupce Objednatele.

5.6 V případě, že má Dodavatel na svých nosičích Data vysoké či kritické úrovně dle přílohy č. 1 VKB, má povinnost tuto skutečnost nejpozději při ukončení Smlouvy oznámit Objednateli a dle volby Objednatele tyto nosiče fyzicky zlikvidovat protokolárně nebo je předat k likvidaci Objednateli.

5.7 Další pravidla pro využití Dat stanoví Smlouva.

6. ŘÍZENÍ RIZIK

6.1 Před zahájením poskytování plnění dle Smlouvy Dodavatel zajistí:

6.1.1 identifikaci aktiv v rámci předmětu plnění Smlouvy a jejich kategorizaci, hodnocení a zařazení do bezpečnostních úrovní v souladu s § 4 a přílohou č. 1 VKB;

6.1.2 identifikaci a hodnocení relevantních hrozeb a zranitelností pro aktiva dle odst. 6.1.1 se zohledněním kategorie hrozeb a zranitelností uvedených v příloze č. 3 VKB a v rozsahu dle přílohy č. 2 VKB;

6.1.3 zpracování prohlášení o aplikovatelnosti pro aktiva dle odst. 6.1.1 podle § 5 odst. 1 písm. f) VKB; a

6.1.4 zpracování plánu zvládání rizik pro aktiva dle odst. 6.1.1 podle § 5 odst. 1 písm. g) a h) VKB.

6.2 Při provádění úkonů podle odst. 6.1 této Přílohy je Dodavatel povinen postupovat podle metodik a postupů a se zohledněním podkladů od Objednatele, byly-li mu

Objednatelem za tímto účelem poskytnuty, pokud mu poskytnuty nebyly, pak za dodržení metodik a postupů dle ISO/IEC/IEEE 15289, ISO/IEC/IEEE 26511, ISO/IEC/IEEE 26512, ISO/IEC 26513 a ISO/IEC/IEEE 26515.

6.3 Úkony podle odst. 6.1 této Přílohy zajistí Dodavatel nejméně jednou ročně a dále pokud nastanou okolnosti podle § 5 odst. 1 písm. h) VKB.

6.4 Smluvní strany se zavazují podrobit předání a převzetí dokumentace podle odst. 6.1 této Přílohy akceptačnímu řízení, které proběhne za podmínek dle Smlouvy, přičemž lhůta pro připomínkování dokumentů a lhůta k odstranění vad dokumentů se stanoví v tomto případě na 10 pracovních dnů. Nestanoví-li Smlouva pravidla akceptačního řízení, má Objednatel ve lhůtě pro připomínkování dokumentů právo vytknout Dodavateli vady dokumentů. Dokument má vadu, je-li v rozporu s požadavky ZKB, VKB nebo Smlouvy (vč. této Přílohy) nebo má navržený postup negativní dopad do bezpečnosti informací. Dodavatel je povinen ve lhůtě k odstranění vad dokumentů předat Objednateli dokumenty bez vad vytknutých Objednatelem, pokud tato lhůta není ve Smlouvě, pak je 10 pracovních dnů. Tato procedura se může opakovat, nejsou-li vady dokumentů odstraněny řádně.

6.5 Dodavatel je povinen zavést a po celou dobu trvání Smlouvy udržovat opatření dle aktuálního plánu zvládání rizik podle odst. 6.1.4 této Přílohy. Opatření je Dodavatel povinen zavést před zahájením poskytování plnění dle Smlouvy. Zejména je Dodavatel povinen zavést a udržovat opatření v oblasti:

6.5.1 klasifikace informací,

6.5.2 nakládání s informacemi,

6.5.3 školení pracovníků Dodavatele v IT bezpečnosti,

6.5.4 přístupu k logům a auditním stopám,

6.5.5 mobilních zařízení a práce na dálku (VPN),

6.5.6 řízení přístupů,

6.5.7 centrálního řízení bezpečnostních nastavení,

6.5.8 kryptografických bezpečnostní opatření,

6.5.9 fyzické bezpečnosti,

6.5.10 ukládání dat,

6.5.11 dostupnosti dat,

6.5.12 zálohování,

6.5.13 správy zranitelností a záplat,

6.5.14 ochrany před škodlivým softwarem a

6.5.15 vývoje a údržby systémů,

v souladu s Pravidly pro dodavatele a bezpečnostními politikami, které jsou dále rozvedeny v této Příloze Smlouvy.

7. NAKLÁDÁNÍ S INFORMACEMI

7.1 Dodavatel se zavazuje pro klasifikaci informací užívat stupně klasifikace Objednatele, pokud mu byly sděleny, nebo je povinen zavést vlastní mapování či překlad rizik mezi klasifikačním schématem a klasifikací Objednatele.

7.2 Dodavatel je povinen zavést vhodná opatření pro ochranu informací přiměřené úrovni jejich klasifikace.

7.3 Dodavatel nesmí používat nebo sdílet informace Objednatele pro jiné účely, než jsou vymezeny ve Smlouvě.

7.4 Dodavatel je povinen omezit přístup k informacím Objednatele pouze na ty zaměstnance a třetí strany, u kterých přístup vyžaduje plnění Smlouvy nebo plnění zákonných povinností. Dodavatel nesmí umožnit přístup k informacím Objednatele jiným organizacím, jako například poddodavatelům nebo partnerům, bez předcházejícího souhlasu Objednatele, který má písemnou formu. Vysloví-li Objednatel ve Smlouvě nebo jinak písemně souhlas se zapojením konkrétního poddodavatele do plnění Smlouvy, uděluje tím souhlas se zpřístupněním informací Objednatele poddodavateli v rozsahu nezbytném pro plnění Smlouvy.

7.5 Učiní-li orgány činné v trestním řízení nebo jiné orgány státní správy jakoukoli právně závaznou žádost o poskytnutí informací Objednatele, je Dodavatel povinen tuto skutečnost oznámit Objednateli s předstihem před poskytnutím takových informací, pokud mu to právní předpisy nezakazují.

8. ŘÍZENÍ PŘÍSTUPU

8.1 Zásady řízení přístupu jsou uvedeny dále v tomto odst. 8.1.

8.1.1 Politika řízení přístupů by měla být nastavena, dokumentována, a revidována na základě business požadavků a požadavků informační bezpečnosti tak, aby efektivně chránila důvěrnost, dostupnost a integritu Dat dle jejich kritičnosti/citlivosti.

8.1.2 Kontrola pokusů o neoprávněný přístup k citlivým IT komponentům by měla probíhat alespoň jednou ročně.

8.1.3 Dodavatel je povinen zajistit, že součástí každé aplikace je funkce řízení přístupu odpovídající kritičnosti zpracovávaných informací.

8.1.4 Účty musí být vytvářeny výhradně pro fyzické osoby a výhradně fyzickými osobami využívány. Jedinou výjimkou jsou technické účty.

8.1.5 Sdílené uživatelské účty, tedy účty, které má používat skupina lidí, by neměly být vytvářeny, protože neumožňují přiřazení individuální odpovědnosti. Nemělo by být k dispozici anonymní používání systémů a služeb nebo používání sdílených účtů.

8.1.6 Výchozí nebo dočasná hesla musí být změněna při prvním použití uživatelem. Individuální heslo uživatele musí být uchováno v tajnosti.

8.1.7 Hesla, uživatelské účty a šifrovací klíče nesmí být nijak a s nikým sdíleny, např. telefonicky, e-mailem nebo jakýmkoliv jiným způsobem.

8.1.8 Po deseti neúspěšných pokusech o přihlášení musí být účet zamčen.

8.1.9 Dodavatel musí monitorovat užívání sítí, služeb, aplikací a dat, aby byl schopen zjistit neoprávněný přístup a zamezit mu. Aktivity administrátorů by měly být logovány a logy by měly být chráněny před změnou nebo neoprávněným přístupem.

8.1.10 Používání nepersonifikovaných účtů (např. “root” nebo “správce”) je dovoleno pouze v případě, že není z technických důvodů jiná možnost. V tomto případě musí být přístup k takovým účtům monitorován, a jakékoli jeho neoprávněné užití musí být ztíženo častější změnou hesla (nejméně jednou za měsíc).

8.2 Role řízení přístupů jsou uvedeny dále v tomto odst. 8.2.

8.2.1 Dodavatel je povinen implementovat oddělení povinností u rolí nejméně na:

8.2.1.1 podávání žádostí o přístup,

8.2.1.2 udílení přístupů a

8.2.1.3 správu přístupů.

8.2.2 Řízení přístupů by mělo být řešeno na základě rolí.

8.3 Politika řízení přístupů je uvedena dále v tomto odst. 8.3.

8.3.1 Politika řízení přístupů musí být revidována a aktualizována nejméně jednou za rok. Politika musí odpovídat legislativním a smluvním požadavkům.

8.3.2 Politika řízení přístupů by měla požadovat:

8.3.2.1 Schvalování žádostí uživatelů o přístup vlastníkem aktiva.

8.3.2.2 Oddělení neslučitelných povinností.

8.3.2.3 Přístup na základě principu “need to know”.

8.3.2.4 Zachování principu “deny by default”.

8.3.2.5 Privilegovaná přístupová oprávnění.

8.3.2.6 Pravidla pro sdílené uživatelské účty.

8.3.2.7 Revize přístupových oprávnění.

8.3.2.8 Odebírání přístupových oprávnění.

8.3.2.9 Vícefaktorovou autentizaci při přístupu k citlivým IT komponentám nebo vzdáleném přístupu k datům Objednatele.

8.4 Přihlašování a pravidla přístupů jsou uvedena dále v tomto odst. 8.4.

8.4.1 Hesla defaultních účtů musí být změněna během úvodního nastavení. Přiřazená hesla musí splňovat minimální bezpečnostní požadavky tak, aby efektivně chránila důvěrnost, dostupnost a integritu informací, ke kterým má Dodavatel přístup, dle jejich kritičnosti/citlivosti.

8.4.2 Zamykání obrazovky a klávesnice (např. spořič obrazovky zamčený heslem) musí být používáno, umožňuje-li to operační systém používaných IT komponent.

8.4.3 Musí být zavedeny postupy pro odebírání nebo blokování přístupových oprávnění uživatelů po ukončení jejich pracovního poměru nebo jiné formy

spolupráce, aby bylo zajištěno, že účty ve všech systémech, ke kterým měl uživatel přístup, jsou bezodkladně zablokovány.

8.4.4 Všechny IT komponenty musí být před předáním uživatelům konfigurovány tak, aby citlivé bezpečnostní operace mohly vykonávat pouze osoby s příslušným oprávněním (správci). O výjimkách musí být informována příslušná osoba Objednatele. Výjimky musí být předem schváleny a zdokumentovány.

8.4.5 Dále musí být zavedeny postupy pro odebírání nebo blokování přístupových oprávnění uživatelů po ukončení jejich pracovního poměru, kontraktu, nebo jiné dohody, aby bylo zajištěno, že:

8.4.5.1 přístupová oprávnění k vybavení a službám zpracování dat jsou bezodkladně odebírána a / nebo

8.4.5.2 přihlašovací údaje (např. ID uživatele, heslo, token nebo digitální certifikát) jsou bezodkladně zablokované a / nebo

8.4.5.3 komponenty, které umožňují přístup, jako jsou tokeny nebo identifikační karty zaměstnanců, jsou bezodkladně zablokovány nebo deaktivovány v systému.

8.4.6 Dodavatel může být Objednatelem požádán, aby mu poskytnul podporu při provádění auditu uživatelských oprávnění v systémech pod kontrolou Dodavatele. Dodavatel musí poskytnut podporu, která bude pro tento účel potřebná.

9. DOKUMENTACE

9.1 Dodavatel je povinen zpracovat a do 20 pracovních dnů od zahájení poskytování plnění dle Smlouvy Objednateli předat dokumentaci, která bude ve smyslu přílohy č. 5 VKB zahrnovat:

9.1.1

9.1.2 postupy pro řízení provozu a komunikací;

9.1.3 postupy pro řízení přístupů (konkrétní postupy pro pracovníky Dodavatele a jeho poddodavatelů podílející se na poskytování plnění dle Smlouvy);

9.1.4 postupy pro bezpečné chování uživatelů (konkrétní postupy pro pracovníky Dodavatele a jeho poddodavatelů podílející se na poskytování plnění dle Smlouvy);

9.1.5 postupy pro zálohování a obnovu a dlouhodobé ukládání;

9.1.6 postupy pro řízení technických zranitelností;

9.1.7 postupy pro zajištění bezpečnosti komunikační sítě;

9.1.8 postupy pro ochranu před škodlivým kódem;

9.1.9 postupy pro nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

9.1.10 postupy pro bezpečné používání kryptografické ochrany

9.1.11 postupy pro řízení změn;

9.1.12 postupy pro zvládání incidentů;

9.1.13 pro řízení kontinuity činnosti;

9.1.14 přehled jednotlivých zařízení pro poskytovanou službu (v rozsahu konfiguračních údajů CMDB aktualizovaných na denní bázi: obecný název, typ zařízení, označení výrobce, sériové číslo, ID/tag, typ HW včetně verze, typ SW včetně verze, typ a počet CPU, velikost RAM, výrobcem udávaný příkon, řešitelská skupina odpovědná za zařízení, emailový a telefonický kontakt na řešitelskou skupinu odpovědnou za zařízení);

9.1.15 další dokumentaci relevantní pro poskytování služby (přehled topologie infrastruktury pro poskytovanou službu; konfigurační standard včetně nastavení zabezpečení pro jednotlivá zařízení minimálně v takovém rozsahu, aby dle něj bylo možné nastavit nové zařízení v případě havárie); a

9.1.16 další požadavky dle Přílohy č. 1 Smlouvy a jejích příloh.

9.2 Nejsou-li požadavky na obsah konkrétní části dokumentace podle odst. 9.1 této Přílohy stanoveny VKB, ZKB, Smlouvě (vč. této Přílohy) ani výkladovém dokumentu Národního úřadu pro kybernetickou a informační bezpečnost, uplatní se pro zpracování dokumentace příměřně požadavky mezinárodně platných technických norem, zejména ISO/IEC/IEEE 15289, ISO/IEC/IEEE 26511, ISO/IEC/IEEE 26512, ISO/IEC 26513 a ISO/IEC/IEEE 26515.

9.3 Dokumentaci podle odst. 9.1 této Přílohy je Dodavatel povinen revidovat a případně aktualizovat nejméně jednou ročně a dále kdykoli při změně skutečností zachycených v dokumentaci. Dodavatel je povinen výsledek provedené revize a případné aktualizace oznámit Objednateli bez zbytečného odkladu od jejich provedení.

9.4 Smluvní strany se zavazují podrobit předání a převzetí dokumentace podle odst. 9.1 této Přílohy akceptačnímu řízení, které proběhne za podmínek dle Smlouvy, přičemž lhůta pro připomínkování dokumentů a lhůta k odstranění vad dokumentů se stanoví v tomto případě na 10 pracovních dnů. Nestanoví-li Smlouva pravidla akceptačního řízení, má Objednatel ve lhůtě pro připomínkování dokumentů právo vytknout Dodavateli vady dokumentů. Dokument má vadu, je-li v rozporu s požadavky ZKB, VKB nebo Smlouvy (vč. této Přílohy) nebo má navržený postup negativní dopad do bezpečnosti informací. Dodavatel je povinen ve lhůtě k odstranění vad dokumentů předat Objednateli dokumenty bez vad vytknutých Objednatelem, pokud tato lhůta není ve Smlouvě, pak je 10 pracovních dnů. Tato procedura se může opakovat, nejsou-li vady dokumentů odstraněny řádně.

10. PROVÁDĚNÍ AUDITŮ

10.1 Není-li ve Smlouvě stanoveno jinak uplatní se na provádění auditů tento článek 10.

10.2 Dodavatel umožní, na základě předchozí výzvy ze strany Objednatele doručené v přiměřeném časovém předstihu a pouze v nezbytném rozsahu, přístup k údajům, účtům, záznamům, pracovním postupům, technické dokumentaci, jiným dokladům či podkladům, k aktivům, do prostor (včetně kontroly fyzického perimetru) a k technickým prostředkům vztahujícím se k plnění Smlouvy a této Přílohy, a to za účelem uskutečnění auditu provozních a technologických procesů, bezpečnostních opatření používaných Dodavatelem při plnění povinností vyplývajících ze Smlouvy a této Přílohy a/nebo při plnění povinností dle této Přílohy (dále jen "**Audit**").

10.3 Audit bude prováděn dle potřeb Objednatele, a to v pravidelných intervalech a v případě bezpečnostních událostí, důvodného podezření na nedostatečnou úroveň ochrany Dat či důvodného podezření na nakládání s Daty v rozporu s relevantními ustanoveními Smlouvy.

10.4 Audit bude prováděn Objednatelem nebo jím pověřeným externím auditorem, smluvně zavázaným k mlčenlivosti minimálně v rozsahu odpovídajícím povinnostem mlčenlivosti Objednatele dle Smlouvy.

10.5 Dodavatel poskytne veškerou nezbytnou součinnost k řádnému provádění a dokončení Auditu a pro tuto činnost zajistí účast kvalifikovaných pracovníků.

10.6 Jakákoliv data, informace nebo jiná aktiva získaná při Auditu mohou být použita výhradně pro účely Auditu či penetračního testování dle čl. 11 této Přílohy, vyhodnocení jejich výsledků a přijetí navazujících opatření, a další potřeby Objednatele při řízení vztahu s Dodavatelem.

10.7 Součást ceny za plnění dle Smlouvy tvoří také náklady na provedení jednoho Auditu za rok. Náklady na provedení Auditu nad rozsah uvedený v předchozí větě nese Objednatel v tom případě, že Audit neodhalí podstatné porušení povinností dle Smlouvy ani bezprostřední hrozby takového podstatného porušení. Pokud Audit odhalí jakékoliv podstatné porušení nebo hrozbu takového podstatného porušení, uhradí Dodavatel Objednateli veškeré důvodně vynaložené náklady vzniklé v důsledku Auditu a porušení bezodkladně napraví vč. případné implementace dodatečných bezpečnostních opatření. Dodavatel je povinen bez zbytečného odkladu, nejpozději však do 10 dní povinen informovat Objednatele a doložit mu splnění povinností dle předchozí věty, včetně uvedení konkrétních opatření, které přijal k odstranění závadného stavu.

11. PENETRAČNÍ TESTOVÁNÍ

11.1 Není-li ve Smlouvě stanoveno jinak, uplatní se na provádění penetračního testování tento článek 11 Přílohy.

11.2 Dodavatel je povinen strpět a poskytnout v souladu s Pravidly pro dodavatele a bezpečnostními politikami součinnost při provádění pravidelného a ad-hoc penetračního testování.

11.3 Penetrační testování bude prováděno Objednatelem nebo jím pověřeným dodavatelem Objednatele, nad rámec penetračních testů prováděných Dodavatelem, a to jak v rámci jednotlivých dílčích etap dodání EMS II, tak jako součást akceptační procedury.

11.4 Všechny osoby zapojené do penetračního testování musejí být zavázány k mlčenlivosti ve vztahu k důvěrným informacím, a to minimálně v rozsahu odpovídajícím povinnostem mlčenlivosti Objednatele dle Smlouvy.

11.5 Jakákoliv data, informace nebo jiná aktiva získaná při penetračním testování mohou být použita výhradně pro účely Auditu či penetračního testování, vyhodnocení jejich výsledků a přijetí navazujících opatření.

11.6 Součást ceny za plnění dle Smlouvy tvoří také náklady na součinnost Dodavatele při provedení jednoho penetračního testování za rok. Náklady na provedení penetračního testování nad rozsah uvedený v předchozí větě nese Objednatel v tom případě, že penetrační testování neodhalí podstatné porušení Smlouvy ani bezprostřední hrozbu

takového podstatného porušení. V případě, že penetrační testování odhalí jakékoliv podstatné porušení Smlouvy nebo bezprostřední hrozbu takového podstatného porušení, uhradí Dodavatel Objednateli veškeré důvodně vynaložené náklady vzniklé v důsledku penetračního testování a zjištěné porušení či hrozby porušení odstraní bez zbytečného odkladu.

12. ŘÍZENÍ ZMĚN

12.1 Dodavatel je povinen nejpozději při zahájení poskytování plnění dle Smlouvy zavést a po dobu trvání Smlouvy udržovat ve vztahu k plnění dle Smlouvy proces řízení změn vymezený v souladu s § 11 VKB, který zejména zajistí, že Dodavatel:

12.1.1 posoudí, zda změna ve vztahu k plnění dle Smlouvy je významnou změnou ve smyslu § 2 písm. o) VKB;

12.1.2 posoudí rizika související s významnou změnou ve vztahu k plnění dle Smlouvy, testuje změnu před nasazením do provozu a posoudí možnost případného navrácení do původního stavu;

12.1.3 přijme přiměřená opatření ke zvládání rizik souvisejících s touto změnou, nebo změnu vůbec neprovede, pokud nelze přijmout opatření snižující tato rizika na akceptovatelnou úroveň; a

12.1.4 dokumentuje posouzení rizik souvisejících s významnou změnou ve vztahu k plnění dle Smlouvy a přijatá opatření.

12.2 Řízení a evidence změn bude probíhat v nástroji Objednatele specifikovaném v Pravidlech pro dodavatele a bezpečnostních politikách. Pokud Dodavatel používá pro řízení změn vlastní nástroj, zajistí přenesení požadovaných informací z tohoto nástroje do nástroje Objednatele.

13. INFORMAČNÍ POVINNOST DODAVATELE

13.1 Dodavatel je povinen Objednatele bez zbytečného odkladu informovat o:

13.1.1 identifikovaných kybernetických bezpečnostních incidentech souvisejících s plněním Smlouvy, nejpozději však do 48 hodin od jejich výskytu;

13.1.2 způsobu řízení rizik na straně Dodavatele a o zbytkových rizicích souvisejících s plněním Smlouvy;

13.1.3 významné změně ovládání Dodavatele, přičemž ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení, a to do 5 pracovních dnů od uskutečnění této změny; a

13.1.4 o změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, a to do 5 pracovních dnů od uskutečnění této změny,

přičemž k informování využije Dodavatel nástroj Objednatele specifikovaný v Pravidlech pro dodavatele a bezpečnostních politikách či jiný prostředek dle písemného pokynu Objednatele.

13.2 Zásadními aktivy dle odst. 13.1.4 a odst. 17.2 této Přílohy jsou zejména aktiva, s pomocí nichž je možné přímo či nepřímo ovlivňovat bezpečnost systému a informací

v něm obsažených, tedy aktiva, kterými proudí informace Objednatele či skrze která je možné proniknout do jeho systémů a která jsou zásadní pro realizaci Smlouvy.

14. PROCES UKONČENÍ SMLOUVY A ŘÍZENÍ KONTINUITY ČINNOSTÍ

14.1 Není-li ve Smlouvě stanoveno jinak uplatní se na pravidla pro ukončení Smlouvy a řízení kontinuity tento článek 14.

14.2 Dodavatel se ve vztahu k poskytování plnění dle Smlouvy zavazuje zavést a udržovat opatření pro zajištění kontinuity činností ekvivalentní k opatřením dle normy ISO 22301 vč. opatření blíže stanovených v Pravidlech pro dodavatele a bezpečnostních politikách. Zejména se Dodavatel zavazuje:

14.2.1 zajistit adekvátní kontinuitu aktiv, která jsou potřebná k poskytování plnění dle Smlouvy; a

14.2.2 pravidelně kontrolovat a testovat, že je Dodavatel schopen zajistit kontinuitu aktiv při dodržení sjednané úrovně plnění dle Smlouvy.

14.3 Dodavatel se zavazuje poskytnout nezbytnou součinnost při zpracování a testování plánů obnovy a havarijních plánů a plnění dalších povinností Objednatele dle § 15 VKB.

14.4 Dodavatel se zavazuje seznámit s pravidly pro řízení kontinuity Objednatele, jak jsou specifikována v této Příloze a Pravidlech pro dodavatele a bezpečností politice.

14.5 Smluvní strany se dohodly, že při ukončení Smlouvy z jakéhokoli důvodu vyvinou veškeré úsilí k tomu, aby do doby dokončení migrace Dat či převodu plnění dle Smlouvy k Objednateli nebo jinému provozovateli, nedošlo k narušení parametrů plnění ve Smlouvě do té doby definovaných, a aby případný nový provozovatel dostal veškeré informace o plnění Smlouvy potřebné pro pokračování nebo nahrazení takového plnění.

15. SMLUVNÍ POKUTA

15.1 V případě porušení jakékoli povinnosti Dodavatele dle této Přílohy, je Objednatel oprávněn požadovat smluvní pokuty, jak jsou vymezeny níže, a to za každé jednotlivé porušení, nestanoví-li Smlouva za takové porušení smluvní pokutu vyšší. Objednatel je oprávněn požadovat pokuty v případě, že:

15.1.1 došlo k porušení této Přílohy Dodavatelem, a to ve výši 250.000 Kč;

15.1.2 došlo k porušení této Přílohy Dodavatelem, přičemž toto porušení vedlo ke kybernetickému bezpečnostnímu incidentu, a to ve výši 500.000 Kč;

15.1.3 došlo k porušení této Přílohy Dodavatelem a dané nedostatky nebyly Dodavatelem odstraněny a negativní následek porušení jeho povinnosti dle této Přílohy stále trvá, a to ve výši 10.000 Kč za každý započatý den;

15.2 . Smluvní pokutou není dotčeno právo Objednatele požadovat náhradu škody ve výši převyšující zaplacenou smluvní pokutu.

16. DODATEČNÁ BEZPEČNOSTNÍ OPATŘENÍ

16.1 V případě, že Objednatel při hodnocení rizik spojených s touto Smlouvou identifikuje podstatná rizika, jejichž existence tvoří podstatnou kybernetickou hrozbu a riziko pro předmět této Smlouvy a dosahují kritické úrovně dle přílohy č. 2 VKB, může Objednatel

Dodavateli uložit přijetí dalších bezpečnostních opatření ve smyslu § 5 ZKB bez nutnosti přijetí dodatku Smlouvy ve smyslu § 100 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Objednatel při naplnění podmínek výše předá Dodavateli seznam vybraných bezpečnostních opatření, která navrhuje ke snížení identifikovaného rizika zavést, a to včetně konkrétní specifikace formy bezpečnostního opatření. Dodavatel je povinen bez zbytečného prodlení zavést požadovaná bezpečnostní opatření a jejich zavedení oznámit Objednateli. Dodavatel je oprávněn do 5 pracovních dní podat připomínky k formě zvolených bezpečnostních opatření a navrhnout jinou formu zvolených bezpečnostních opatření, kterou je povinen zavést bez zbytečného prodlení, po jejich schválení Objednatelem, a jejich zavedení Objednateli oznámit.

16.2 Další bezpečnostní opatření přijatá dle tohoto článku Přílohy musí být přiměřená, přičemž součást ceny za plnění dle Smlouvy tvoří také náklady na implementaci těchto bezpečnostních opatření, není-li určeno ve Smlouvě jinak.

17. OSTATNÍ UJEDNÁNÍ

17.1 Dodavatel se zavazuje provádět veškerá plnění dle Smlouvy v souladu se Smlouvou, příkazy Objednatele, s předanými podklady a dále v souladu s právními předpisy, zejména ZKB a VKB. Dodavatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy a zajistit ve spolupráci se Objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční nebo efektivní.

17.2 Pokud není ve Smlouvě nebo v této Příloze uvedeno jinak, odměna za provádění opatření dle této Přílohy jsou součástí odměny za Implementaci dle Smlouvy.

17.3 Smluvní strany jsou povinny vzájemně si poskytnout nezbytnou součinnost k tomu, aby řádně naplňovaly právní povinnosti stanovené ZKB a VKB. Jestliže Dodavatel při plnění Smlouvy zjistí či jako odborník mohl a měl zjistit rozpor ustanovení Pravidel pro dodavatele a bezpečností politiky se ZKB, VKB anebo rozhodnutím či jiným pokynem NÚKIB v souladu se ZKB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.

17.4 V případě, že dojde k jakémukoliv rozporu mezi Dodavatelem a třetí osobou, která není jeho poddodavatelem a je dodavatelem software nebo jiných technologií dotčených plněním povinností Dodavatele dle Smlouvy, je Dodavatel povinen tuto skutečnost bez zbytečného odkladu oznámit Objednateli.

17.5 Smluvní strany prohlašují, že je Smlouva včetně jejích příloh v souladu s obecně závaznými právními předpisy, zejména pak se ZKB a VKB.

Příloha č. 8

Seznam poddodavatelů

1/

Název:	Enigma Systemy Ochrony Informacji Sp. z o. o.
Sídlo:	Jutrzenki 116 Street, 02-230 Warsaw, mazovia, Poland
Právní forma:	Společnost s ručením omezeným
Identifikační číslo:	NIP number: 526 10 29 614
Rozsah plnění Smlouvy:	Výroba a dodávka monitorovacích zařízení
	Dodávka softwaru monitorovacího centra
	Účast na procesu předimplementační analýzy
	Účast na integraci softwaru monitorovacího centra se systémy zadavatele
	Účast na testech EMS II
	Účast na implementaci EMS II
	Účast na školeních
	Administrace a podpora řízení projektu
	Poskytování provozní podpory třetí linie

Příloha č. 9

Zadávací dokumentace

k dispozici na profilu zadavatele v Národním elektronickém nástroji (NEN) pod ID:
N006/22/V00034083

Příloha č. 10

Vnitřní předpisy Objednatele

(tvoří samostatný dokument v elektronické podobě)