DODATEK Č. 1

LICENČNÍ SMLOUVA

ze dne 9. 7. 2019

(dále jen „**Dodatek č. 1**“)

Smluvní strany:

1. **Centrum kardiovaskulární a transplantační chirurgie**
   se sídlem: 65691 Brno, Pekařská 664/53
   IČO: 00209775
   DIČ: CZ00209775
   zastoupeno: Doc. MUDr. Petrem Němcem, CSc., MBA, ředitelem

   (dále jen „**nabyvatel**“)

   a

2. **C SYSTEM HOLDING s.r.o.**
   se sídlem: Otakara Ševčíka 938/56, 636 00 Brno
   IČO: 28318340
   DIČ: CZ28318340
   zastoupen: [redacted]

   (dále jen „**poskytovatel**“)

(Nabyvatel a Poskytovatel dále společné také jen „**Smluvní strany**“ nebo jednotlivě jako „**Smluvní strana**“)

Dne 9. 7. 2019 uzavřely smluvní strany v souladu s výsledkem veřejné zakázky VZ0065763 – Integrace a garantovaná archivace elektronické zdravotnické dokumentace Licenční smlouvu. Tento Dodatek upravuje práva a povinnosti Smluvních stran souvisejících s dodávkou systému „Rozšíření funkcionality IDM“ a „Úpravy prostředí IP pro „obecná část aplikace“ pro práci s pacientem“. Smluvní strany v souladu se zněním § 222 odst. 5 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, shodně konstatují, že naplňují zákonné podmínky pro změnu závazku ze smlouvy na výše uvedenou veřejnou zakázku.

Na základě zvyšujících se nároků na bezpečnost informačních systémů potřebuje Objednatel zajistit zvýšení bezpečnosti procesu řízení identity zaměstnanců a všech aktérů integrace (díla) a to rozšířením stávajícího řešení IDM. Jedná se především o zajištění bezpečnosti na úrovni efektivní správy identit zaměstnanců, zajištění jejich životního cyklu od předvýběru až po ukončení pracovního poměru zaměstnance, komunikace mezi zapojenými systémy a zavedením centrální správy bezpečnostní politiky.
Díky pořízení rozšiřujícího modulu ke stávajícímu, již implementovanému základnímu systému od stejného výrobce, dojde k výrazné úspoře nákladů na pořízení a provoz celého systému IDM jako celku. Zůstane zachovaná jednotná platforma, jednotná správa, jednotné GUI a společná podpora vývoje i maitenance od jednoho dodavatele řešení.

Pořízení rozšiřujícího modulu IDM od jiného dodavatele by si v budoucnu vyžádalo implementaci jakýchkoliv změn do obou částí řešení IDM, což by generovalo vyšší náklady a rizika spojená s funkčností a zároveň by se tím také zvýšily náklady na správu celého systému.

Existence dvou částí jednoho řešení na různých platformách a jejich těsného propojení je rizikové i z hlediska bezpečnosti zejména v oblasti zálohování, vysoké dostupnosti a zabezpečení proti kyberútoku.

V neposlední řadě, s ohledem na uživatele a administrátory, není také žádoucí, aby byla jedna problematika řešená ve dvou různých uživatelských rozhraních.

Dále v současné době Objednavatel používá několik samostatných aplikací (agend) vytvořených v různých prostředích. Tyto jednoúčelové aplikace nemají žádnou vazbu na nově budované integrační prostředí. Implementací požadovaných rozšíření získá Objednavatel možnost využití plné integrace pro převedení stávajících agend a tvorbu nových kompozitních aplikací s využitím služeb MPI, Document registry, generátoru lineárních 1D a 2D kódů, centrálních číselníků a IDM.

Článek I.
Úvodní ustanovení

1. Smluvní strany uzavřely dne 9. 7. 2019 Licenční smlouvu

2. Smluvní strany se dohodly prostřednictvím tohoto Dodatku č. 1. na níže uvedené změně předmětné smlouvy.

Článek II.
Změna Smlouvy

1. Smluvní strany se dohodly na změně čl. 2 „Předmět smlouvy“, který se tímto mění následovně v bodě 2.1.1.:
   „2.1.1. dodat dílo, který tvoří dodávka a vybudování integrační platformy Poskytovatelem pro Nabyvatele na architektuře ESB, která umožní napojení současných systémů a aplikací včetně získávání a systematického ukládání dat. Hlavními součástmi řešení budou dále Master Patient Index, centrální registr zdravotnické dokumentace, Systém pro správu identit (dále IDM) a dlouhodobý důvěryhodný archiv elektronické zdravotnické dokumentace.“

   V návaznosti na výše uvedenou změnu se smluvní strany dohodly na změně čl. 4 Smlouvy „Cena a platební podmínky“, jehož nové znění v bodě 4.2. je následující:
   „4.2. Cena díla činí částku ve výši 14.947.149 Kč bez DPH (slovy: Čtrnáctmilionůděvetsetčtyřicetsedmtisícjednostočtyřicetdevět korun českých). DPH ve výši 21 % činí 3.138.901 Kč slovy: Třimilionystotřicetosmtisícdevětsetjedna korun českých). Cena díla celkem včetně DPH činí 18.086.050 Kč (slovy: Osmnáctmilionůosmdesátšesttisícpadesát korun českých).
   Smluvní strany se dále dohodly na změně přílohy č. 1 Smlouvy – Technická specifikace a Přílohy č. 3 – Položkový rozpočet, jejichž doplněné znění je nedílnou součástí tohoto dodatku.

Článek III.
Závěrečná ustanovení

1. Ostatní ustanovení Smlouvy zůstávají beze změn a v platnosti.

2. Tento Dodatek č. 1 nabývá platnosti dnem podpisu oprávněných zástupců obou Smluvních stran a účinnosti zveřejněním v registru smluv dle zákona č. 340/2015 Sb.

3. Tento Dodatek č. 1 je vyhotoven v elektronické podobě v jednom (1) vyhotovení.

4. Smluvní strany prohlašují, že si tento Dodatek č. 1 přečetly, že s jeho obsahem souhlasí a na důkaz toho k němu připojují svoje podpisy.

Nedílnou součástí tohoto dodatku je:

Příloha č.1 Dodatku – doplněné znění Přílohy č.1 Smlouvy

Příloha č.2 Dodatku – doplněné znění Přílohy č.3 Smlouvy

V Brně dne _____ V Brně dne _____

Příloha č.1 Dodatku – doplněné znění Přílohy č.1 Smlouvy

Doplnění technické specifikace – popis rozšiřujících funkcí díla:

1. „Rozšíření funkcionality IDM“

„Rozšíření funkcionality IDM“ rozšiřuje komponentu „Centrální správa identit uživatelů a oprávnění“ (požadavky P.10.1 a P.10.2 Přílohy č. 1 Smlouvy) o níže popsané funkcionality.

1.1. Specifikace návrhu SW architektury

Kapitola obsahuje popis navrhovaného řešení systému Identity managementu od společnosti C SYSTEM CZ a.s. (dále také „cIDM“) s přihlédnutím k požadavkům zadavatele, jak jsou vyjádřeny v zadávací dokumentaci.

Identity management je chápán jako univerzální systém pro správu identit uživatelských oprávnění v heterogenním informačním systému v rámci podnikové sítě. Výkonné jádrové struktury zachycují stav „zde a nyní“, obsahují vše, co je třeba pro standardní běžnou službu, tedy zejména poskytování seznamů identit a seznamů oprávnění či rolí, dané identity v daném kontextu či v dané doméně. Doménou může být informační systém, budova nebo areál. V rámci domény jsou definovány role pro řízení přístupu.

Systém disponuje možností napojení na zdrojové systémy pro čerpání informací o identitách. Dle dostupných informací může řídit životní cyklus identity od jejího vstoupení v platnost až do ukončení platnosti. V průběhu životního cyklu má uživatel možnost pomocí portálu spravovat svoje základní údaje, které nejsou čerpány ze zdrojových systémů, nahlížet na svoje oprávnění a zvolit na omezenou dobu svého zástupce, nebo delegovat svoje přístupy na jinou identitu.

Systém disponuje grafickým rozhraním pro správce, které umožní nastavení oprávnění pro jednotlivé identity, také automatické přiřazení oprávnění dle definovaných parametrů dostupných v organizační struktuře a zdrojovém systému. Akce prováděné uživateli v systému podléhají logování. Pomocí grafického rozhraní je možné vytvářet reporty pro kontrolu nastavení systému a oprávnění v něm

Systém poskytuje informace o identitách a jejich oprávněních pomocí rozhraní webových služeb SOAP a REST s podporou SSO, OAuth 2 a SAML standardů. Systém umožní napojeným systémům do cIDM vložit rozsah svých podporovaných rolí pro kontrolu integrity. V případě změny v oprávnění uživatele umožní odeslání notifikace napojeným systémům, které si notifikaci „předplatili“.

1.2. Popis architektury řešení Identity managementu

Popis použitých technologií, včetně popisu spuštění systému

Dodávané řešení cIDM není závislé na konkrétním hardware, virtualizační platformě či operačním systému. Navrhované řešení využije těch prvků, které jsou k dispozici, jak jsou popsány v zadávací dokumentaci.

Navrhujeme tedy virtualizační platformu VMware vSphere 6.x operační systém Microsoft Windows min verze 2012 R2 Server Standard, MS IIS 8.5).

Uživatelské prostředí cIDM je budováno pomocí open-source frameworku pro vývoj webových aplikací Angular 11.2.1. Uživatelské rozhraní je ralizováno jako single-page webová aplikace, která běží na koncovém zařízení ve všech standardních webových prohlížečích.

Výkonné jádro cIDM je vybudováno v datové platformě IRIS společnosti InterSystems. Při nasazení předpokládáme verzi InterSystems IRIS for Health 2020.x . InterSystems zajišťuje technickou podporu a aktualizační program pro IRIS, vždy ve spolupráci s dodavatelem aplikace. Tato datová platforma je zároveň integrační platformou zadavatele, na kterou je požadováno napojení v bodu 1.2 technické specifikace. Napojení je takto implicitně zajištěno.

Datová platforma IRIS bude pro cIDM standardním způsobem realizovat:

- databázové prostředí pro všechny typy dat (provozní, konfigurační, dočasná, strukturální atd.)
- běhové prostředí pro skriptovací jazyk pro veškerou databázovou a aplikační logiku
- prostředí pro vývoj objektově orientovaných komponent cIDM, jejich metod a persistentních i transientních vlastností
- prostředí pro vývoj, konfiguraci a provoz všech interoperabilních komponent. (viz *kapitola b Popis integračního rozhraní systému*.)
- IRIS obsahuje rozsáhlý správcovský portál, jehož prostřednictvím bude možné vykonávat nestandardní složité práce, týkající se analýz, auditů, konfigurací a řešení nestandardních situací

Vlastní vývoj dodavatele se týká všech částí a komponent cIDM, s využitím možností a stavebních bloků obsažených ve vývojových a provozních platformách uvedených výše (IRIS, Angular), zejména:

- datových struktur; databázové a aplikační logiky
- komunikačních a integračních komponent; konfigurace adaptérů, tvorba business procesů, služeb a operací, realizujících napojení systému na vnější prostředí

Technická specifikace vrstev systému

Virtualizační platforma dostupná v prostředí zákazníka VMware vSphere s dokumentací dostupnou zde: https://docs.vmware.com/en/VMware-vSphere/index.html

Operační systém Microsoft Windows 2019, MS IIS 10) s dokumentací dostupnou zde: https://docs.microsoft.com/en-us/windows-server

Uživatelské prostředí cIDM je budováno pomocí open-source frameworku pro vývoj webových aplikací Angular 9.1. s dokumentací dostupnou zde: https://v9.angular.io/docs

Výkonné jádro cIDM je vybudováno v datové platformě IRIS společnosti InterSystems. Při nasazení předpokládáme verzi (InterSystems IRIS for Health 2020.x) https://docs.intersystems.com/irisforhealthlatest/csp/docbook/DocBook.UI.Page.cls

Aplikační komponenty, které jsou součástí navrhovaného řešení systému cIDM, jsou popsány dále v tomto dokumentu.

Zabezpečení dat

proti zneužití a poškození se opírá o možnosti poskytované datovou platformou IRIS. Vlastní vývoj cIDM těchto možností využívá, jak uvedeno dále a v žádném případě toto zabezpečení nekompromituje.

Zabezpečení komunikace

Veškerá komunikace platformy s ostatními systémy je zabezpečená prostřednictvím TLS 1.2. Ověřování certifikátů klientských systémů není obecně vyžadováno mimo komunikační kanály, pro které není možná jiná forma autentizace.

Při komunikaci jednotlivých komponent řešení, které jsou nasazené uvnitř zabezpečené sítě a klienta při komunikaci je možné autentizovat jinak než prostřednictvím TLS, není šifrování nutně použito.

Autentizace a autorizace

cIDM zabezpečuje služby autentizace a autorizace, detaily jsou uvedeny dále v nabídce. Těm komponentám, které podporují protokoly IHE, nabízí cIDM služby v souladu s profilem IUA a XUA.

Dle všeobecně doporučovaných postupů umožňuje přihlášení prostřednictvím jednotné přihlašovací stránky a poskytuje napojeným doménám autentizační/autorizační token v souladu s IUA, kdy řešení vystupuje v rolích aktérů Authorization Client a Resource Server podle IUA a autentizace/autorizace probíhá pomocí Authorization Code Grant Flow podle OAuth2. Autentizace/autorizace pro administraci systému pomocí Terminálu je zajištěna prostřednictvím Password Grant podle OAuth2. Také jako X-Service User a X-Service Provider podle profilu XUA (Cross-Enterprise User Assertion). Ne všechny služby tuto úroveň zabezpečení vyžadují/podporují. V takových případech se jedná o komunikaci, která je zabezpečena použitím TLS v1.2 spolu s autentizací pomocí certifikátů, případně ověřením jména a hesla systémového účtu klienta.

Zabezpečení dostupnosti

Zabezpečení dostupnosti se opírá o možnosti poskytované datovou platformou IRIS. Pro zajištění dostupnosti jsou v rámci navrhovaného řešení pro produkční prostředí navrženy 2 webové servery, které umožní load balancing požadavků přicházejících na server.

Zabezpečení důvěrnosti informací

Data jsou chráněna datovou platformou IRIS a zabezpečením komunikačních kanálů, jak je naznačeno výše. Dále je vhodné, aby zadavatel zajistil ochranu databázových a žurnálových souborů platformy, pokud chce zajistit ve svém vnitřním prostředí snížené riziko kompromitování dat

v cIDM. Žurnálování dat je sice možné omezit, v provozním systému by se tím nepřijatelně snížila bezpečnost a dostupnost systému.

- OS – přístup k databázovým souborům by měl být zabezpečen omezením přístupu uživatelů OS k tomuto souboru. Čtení může být povoleno pouze pro systémového uživatele, pod kterým běží procesy IRIS s aplikačním kódem řešení, případně také hlavnímu administrátorovi systému.
- Diskové pole/virtualizace – Kompromitace souborů virtuálních disků virtuálních strojů, na kterých bude nasazeno cIDM, představuje nízké riziko z hlediska čtení dat z databázových souborů existujících v rámci těchto virtuálních disků. Toto riziko je nicméně možné ještě více snížit pomocí šifrování souborů virtuálních disků na úrovni virtualizační vrstvy nebo diskového pole.

Auditní logování

Systém cIDM lze konfigurovat pro zaznamenávání různých typů událostí do zabezpečeného auditního logu. Pokud uživatel disponuje centrálním auditovacím systémem, (například dle IHE profilu ATNA), cIDM jej umí využít a posílat auditovací záznamy do centrálního systému standardizovaným způsobem.

Reporting

V rámci systému lze v čase získávat reporty o stavu systému a jeho nastavení pomocí informačních textů na vyžádání. Pro tyto informační texty lze také nadefinovat jejich odesílání v návaznosti na změny v organizační struktuře a oprávněních.

Mimo výše zmíněnou funkcionalitu disponuje platforma IRIS řadou vestavěných reportů monitorujících stav systému a dostupných prostředků, které se dají spouštět manuálně, nebo dle definovaného časového plánu. Obsah reportu je možné vytvářet na míru různých potřeb organizace.

Zprávy pro včasné varování a zásah

Systém disponuje konfigurovatelnou funkcionalitou informačních textů. V návaznosti na události v rámci životního cyklu entity a organizační struktury je entitě vygenerován informační text, který jí seznámí s rozsahem oprávnění v jednotlivých informačních systémech, která jsou v rámci cIDM definována. Tento text je následně entitě odeslán do její e-mailové schránky. Stejně tak v případě změny v oprávněních, nebo změně vztahu k organizační struktuře je entita informována o jejich změně.

Vlastní provádění notifikace je konfigurovatelné pro příjemce, původce notifikace, správce systému, který je změnou v oprávněních ovlivněn

Pro komunikaci mezi systémy je v rámci cIDM k dispozici mechanismus notifikace řízeného systému, kdy v návaznosti na změny v oprávněních a změny v rámci životního cyklu entit je možné napojeným systémům předávat informace o změnách zasláním identifikátorů uživatelů se

změnou. V návaznosti na tuto notifikaci může napojený systém využít odpovídající služby pro synchronizaci oprávnění uživatele.

Notifikace může napojený systém přijímat pomocí webové služby (REST, SOAP), nebo pomocí souboru.

Notifikace o změnách může probíhat také zasláním celého seznamu oprávněných uživatelů a jejich oprávnění pro daný systém ve formátu CSV, XML

1.3. Popis integračního rozhraní systému

Systém cIDM se připojuje a komunikuje ve dvou záležitostech:
1) cIDM vystupuje jako správce přístupů (Access Manager) a
2) cIDM získává zdrojová a konfigurační data ze zdrojových systémů. Daný systém může komunikovat v obou záležitostech, tedy zároveň poskytovat data (například o uživatelích) a zároveň být řízen z pohledu uživatelských práv.

Access Manager (také Přístupová struktura)

Obecný popis napojení řízeného systému

Komunikace s řízenými systémy probíhá pomocí standardního rozhraní, pomocí kterého systémy konzumují změny v oprávněních a pracovních vztazích, nebo aktualizují celou databázi entit, jejich oprávnění, nebo organizační struktury.

Pro řízené systémy je zřízen konektor, který využívá API daného sytému a umožní jeho řízení přímo z cIDM.

Řízené systému mohou pro nastavení k nim importovat do cIDM jejich strukturu rolí pomocí CSV, nebo XML.

Autentizační mechanismy

Systém disponuje vestavěnými autentizačními mechanismy pro ověření pomocí jména a hesla. Dále umožňuje dalších autentizačních mechanismů v rámci organizace jako jsou autentizace tokenem, pomocí biometrických údajů.

Podporované standardy

OAuth 2.0

OAuth 2.0 (RFC 6749) je moderní autorizační protokol (resp. framework) pro bezpečnou API autorizaci jednoduchým a jednotným způsobem pro webové i desktopové aplikace. Jeho specifikace popisuje podrobně fungování oné výše popsané výměny tokenů a klíčů; nijak nedefinuje vlastní

komunikaci s webovou aplikací ani není vázané na konkrétní typ API (pouze je omezeno na HTTP protokol). OAuth lze tedy použít jako metodu ověření uživatele k jakémukoli typu API (SOAP, XML-RPC, REST atd.), a to nejen na webových aplikacích.

OpenID Connect

Protokol OpenID Connect je nadstavba nad OAuth 2.0 která umožňuje provádět autentizaci uživatelů pro napojené systémy. Podrobnou dokumentaci lze nalézt zde: (https://openid.net/specs/openid-connect-core-1_0.html)

IUA/JWT

IHE profil Internet User Authorization (IUA) definuje konkrétní vlastnosti komunikace a předávaných bezpečnostních tokenů pomocí frameworku OAuth 2.0 pro použití ve zdravotnickém prostředí. Tato rozšíření jsou plně kompatibilní i s protokolem OpenID Connect a lze je tedy vzájemně kombinovat. Specifikace tohoto profilu je dostupná on-line na níže uvedeném odkazu:
https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_IUA.pdf

cIDM podporuje fungování v roli aktéra Authorization Server podle profilu IUA včetně možnosti SAML Token Option.

XUA/SAML

Jako součást autorizačních tokenů bude cIDM klientským systémům předávat i SAML Assertion. Získanou SAML Assertion nesoucí autentizační i autorizační položky pro uživatele mohou klientské systémy následně použít pro autentizaci/autorizaci IHE transakcí podle profilu XUA (https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf#nameddest=3_40_Provide_X_User_Assertion__)

Zdrojové systémy

Obecný princip napojení na zdrojové systémy

Jako zdrojový systém je chápán systém udržující informace o různých entitách v rámci organizace. Těmi mohou být zaměstnanci, dodavatelé, zákazníci, auditoři, systémy hardware a další. Zdrojové systémy můžou dále poskytovat informace o organizační struktuře a vztazích jednotlivých entit k organizační struktuře.

Napojení na zdrojový systém probíhá formou neinvazivní, tudíž provoz zdrojového systému by neměl být narušen napojením cIDM a zátěž na zdrojový systém by měla být co nejmenší. Vlastní napojení je realizováno jak přírůstkovou synchronizací, tak exportem celé databáze uživatelů. Může být realizováno pomocí standartního rozhraní např. LDAP nebo cestou importu souborů ve formátu CSV, XML, JSON resp. využitím voláním webové služby. Dalším ze způsobů napojení je přímé načítání dat z databáze realizované pomocí ODBC driverů nebo podobných řešení.

Mezi základní zdrojové systémy patří:

- Personální systém
- Active Directory

- PKI systém

Konektory systému

Automatické propisování do napojených systému

Komunikace s napojenými systémy probíhá pomocí standardního rozhraní. Jako alternativní způsob napojení systémů lze vytvořit konektor pro jednotlivé systémy, pomocí kterých budou systémy konzumovat změny v oprávněních nebo aktualizovat celou databázi uživatelů a jejich oprávnění.

Konektor může být realizovaný jako:

- napojení na API systému, přes které je možné v systému zakládat uživatele a jejich oprávnění
- vytvoření exportu pro daný systém, který si následně zpracuje.

Systém disponuje možností vytvořit libovolný konektor.

Manuální propisování do napojených systému

Konektory pro systémy, které nejsou schopny konzumovat standardní rozhraní, přijímat informace o entitách pomocí vystavení webové služby ani zpracování exportu, musí být realizovány operátorem/správcem daného systému. Jejich vlastní realizace záleží na dostupných možnostech systému.

Konektor na Active Directory

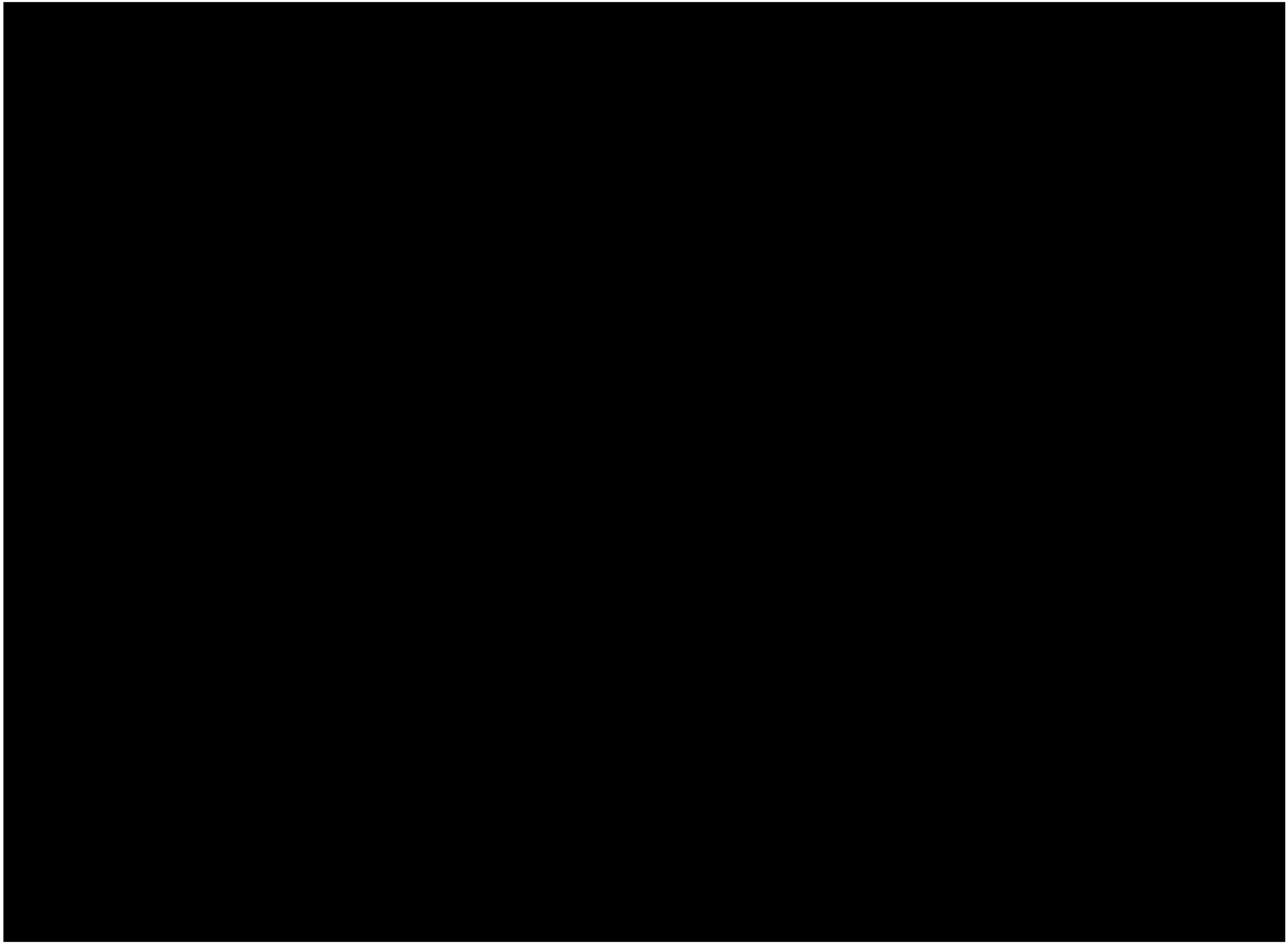
Pro Active Directory disponuje cIDM konektorem umožňujícím základní práci s daty uživatelů jako jsou úpravy informací o uživateli, změna a obnova hesla. Díky tomuto konektoru je umožněna správa skupin v Active Directory a správa vazeb mezi uživatelem a skupinou.

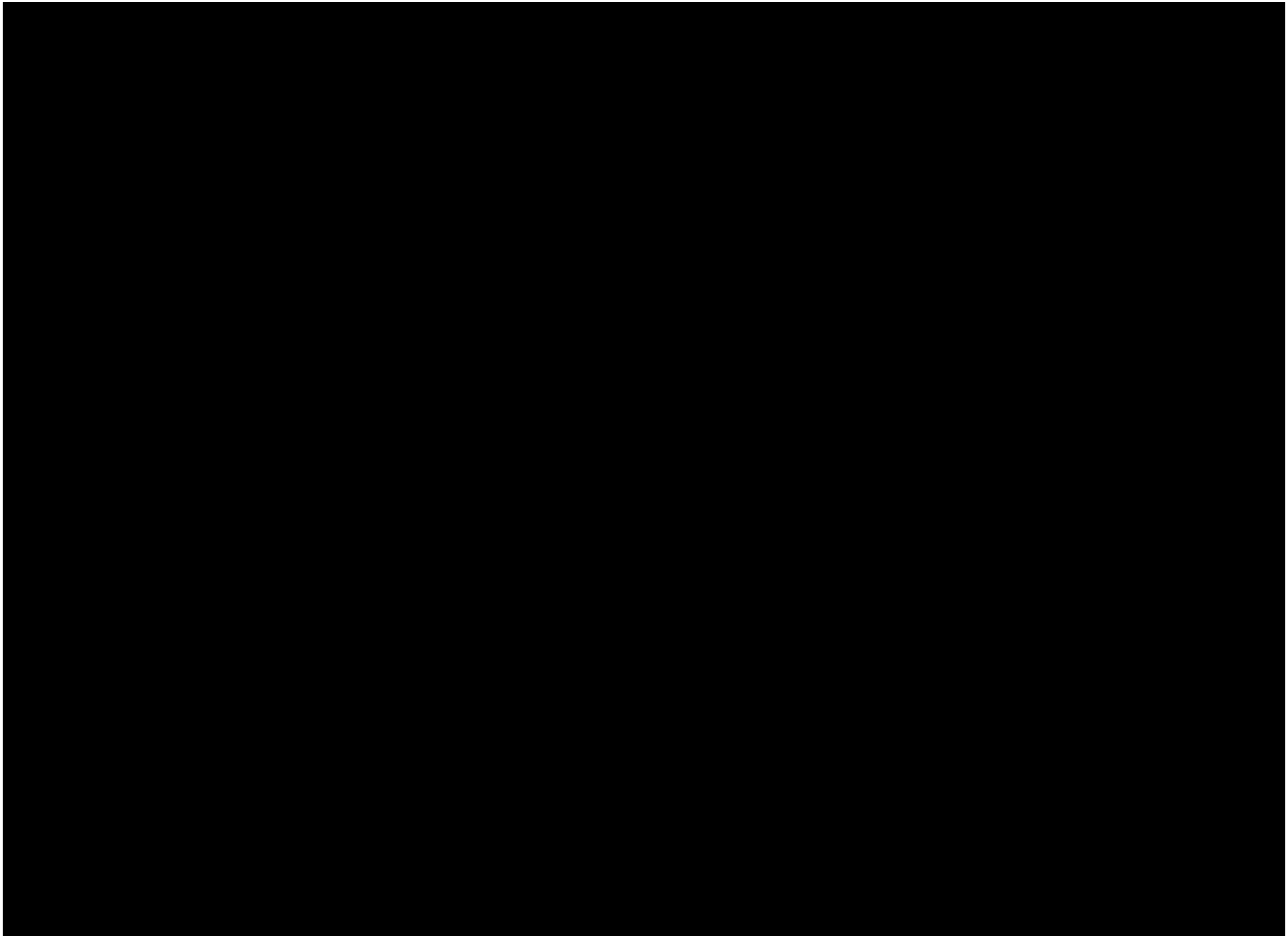
V rámci tohoto konektoru umožňuje cIDM správu přístupu ke sdíleným síťovým prostředkům v rámci systému Windows pro jednotlivé uživatele.

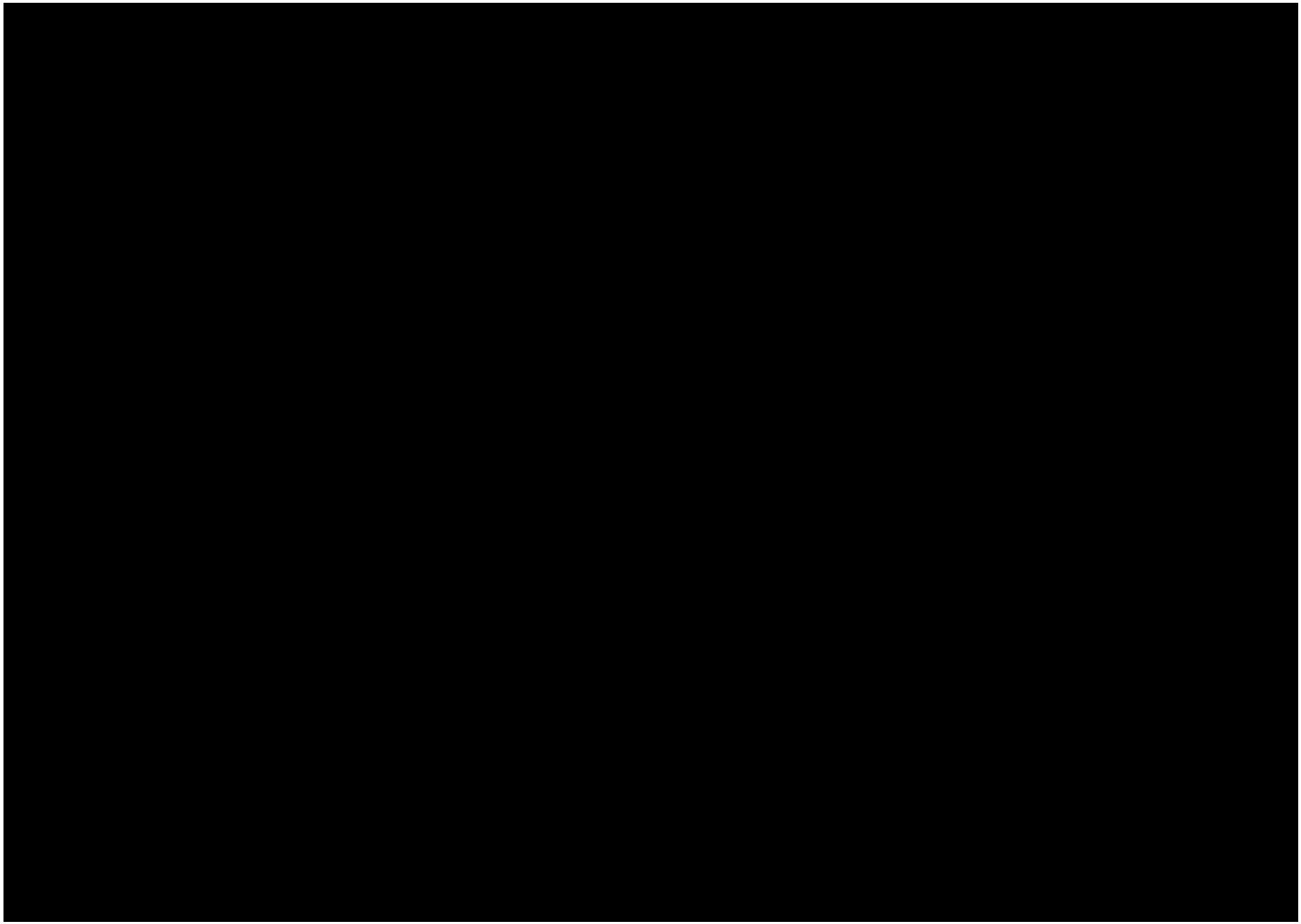
1.4. Nezbytná součinnost zákazníka:

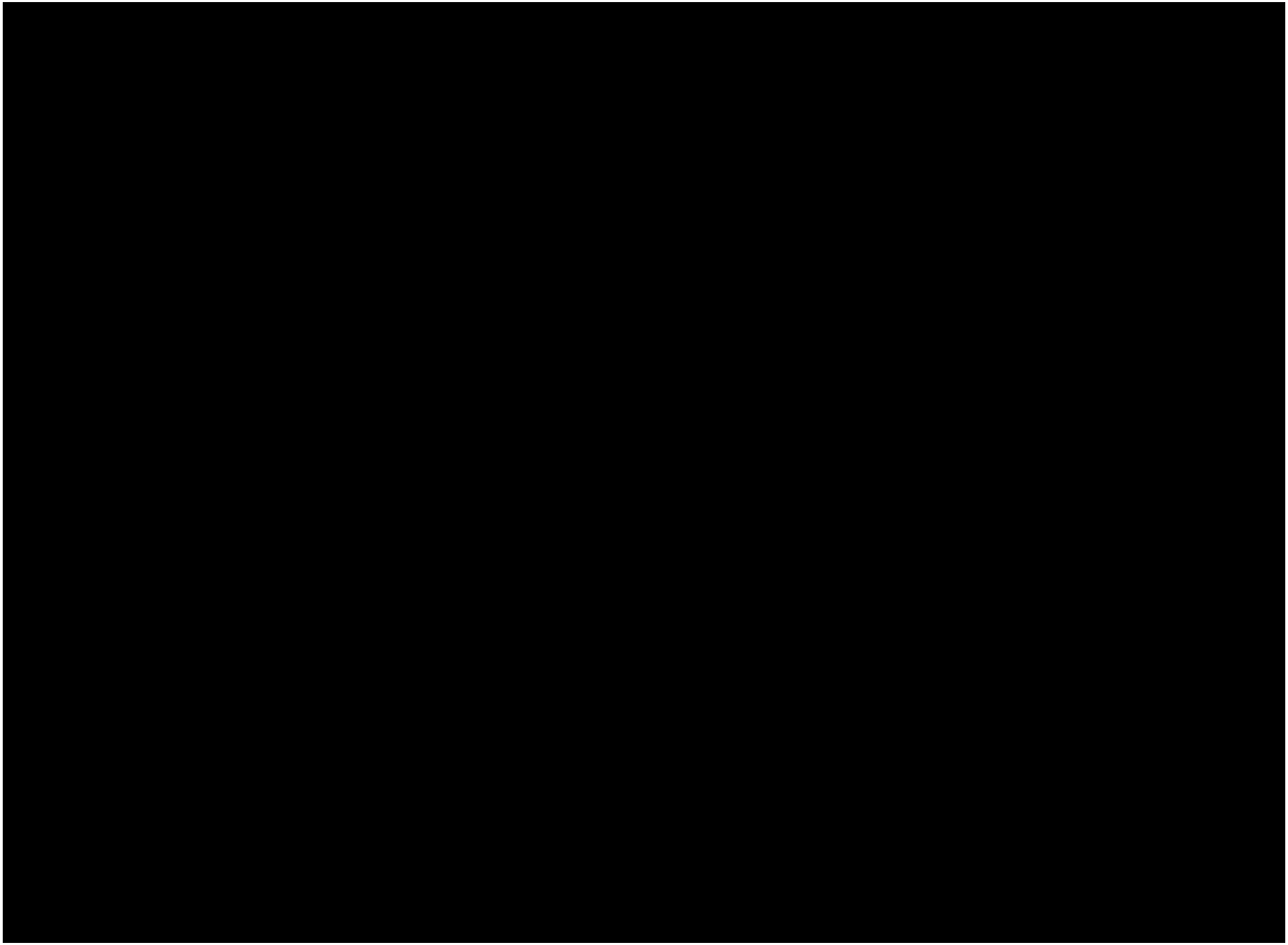
Pro dodávku je nezbytné zajištění součinnosti ze strany zákazníka, a to zejména:

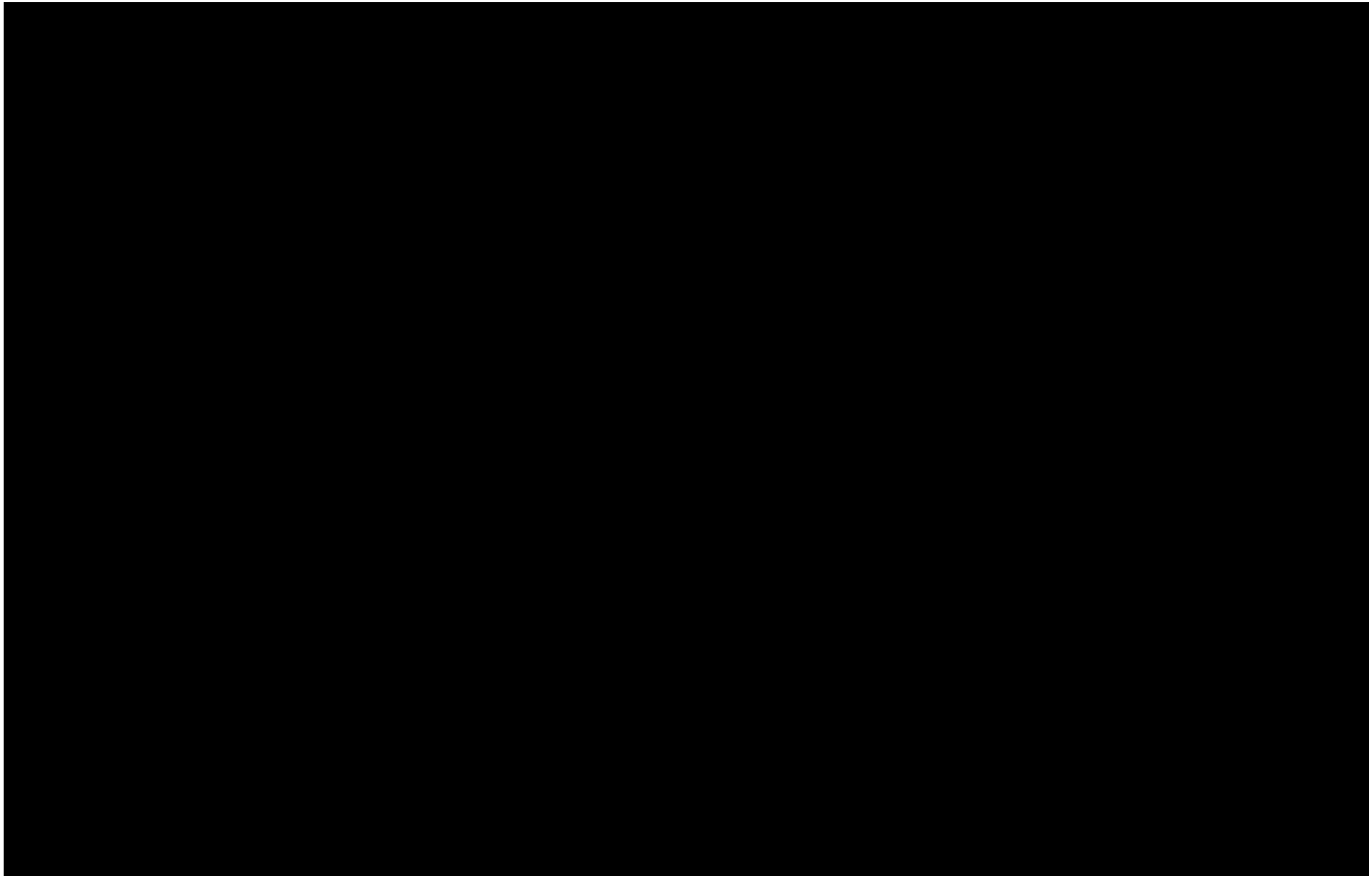
- Výstupy z analýzy potřené pro rozšíření IDM (především napojení na systém VEMA)
- Příprava potřebných rozhraní na straně systémů napojovaných na IDM (systém VEMA)
- Údaje / vstupní data pro naplnění modulu (zdroj dat ze systému VEMA)
- Součinnost při celkovém testování a akceptaci

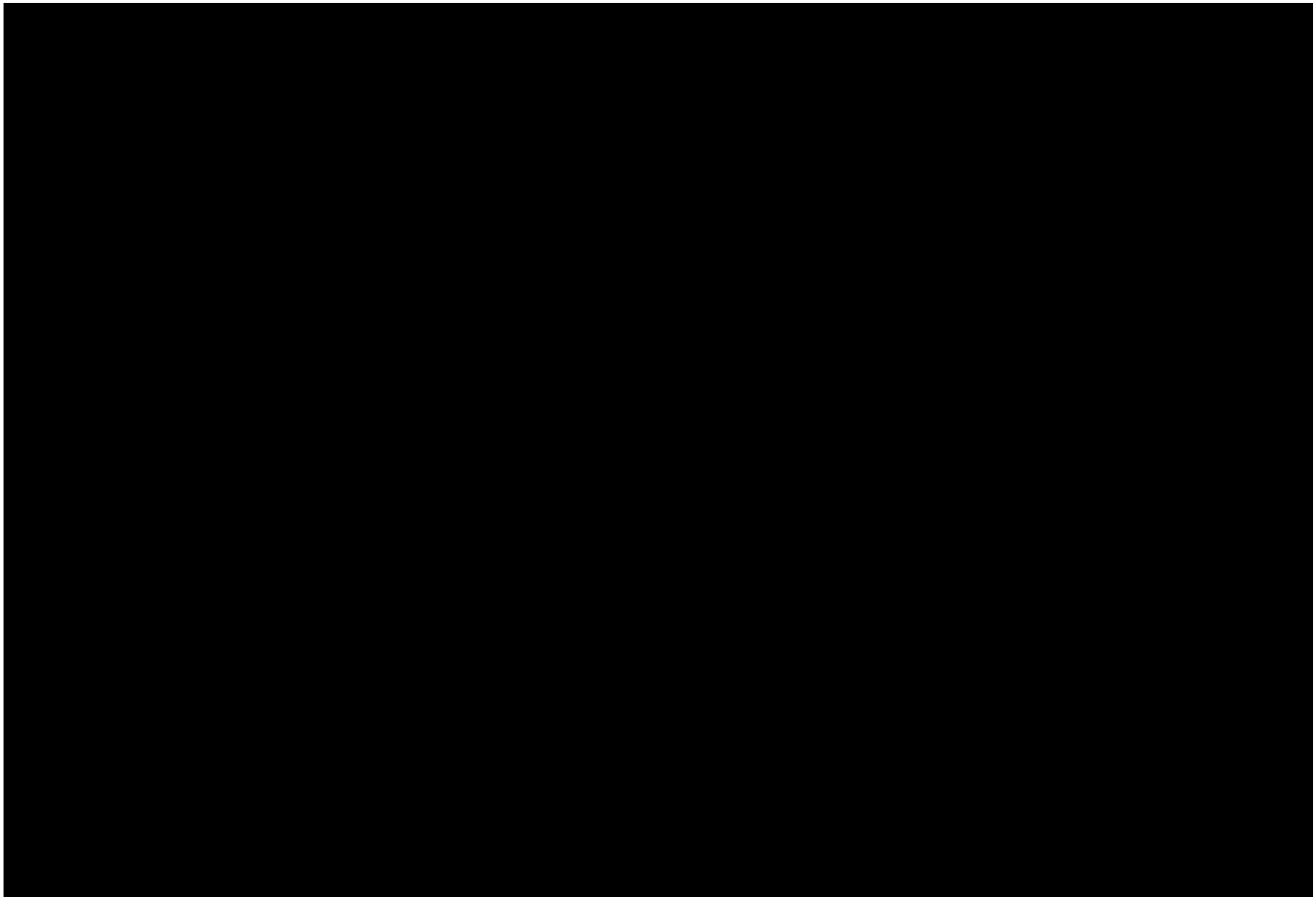


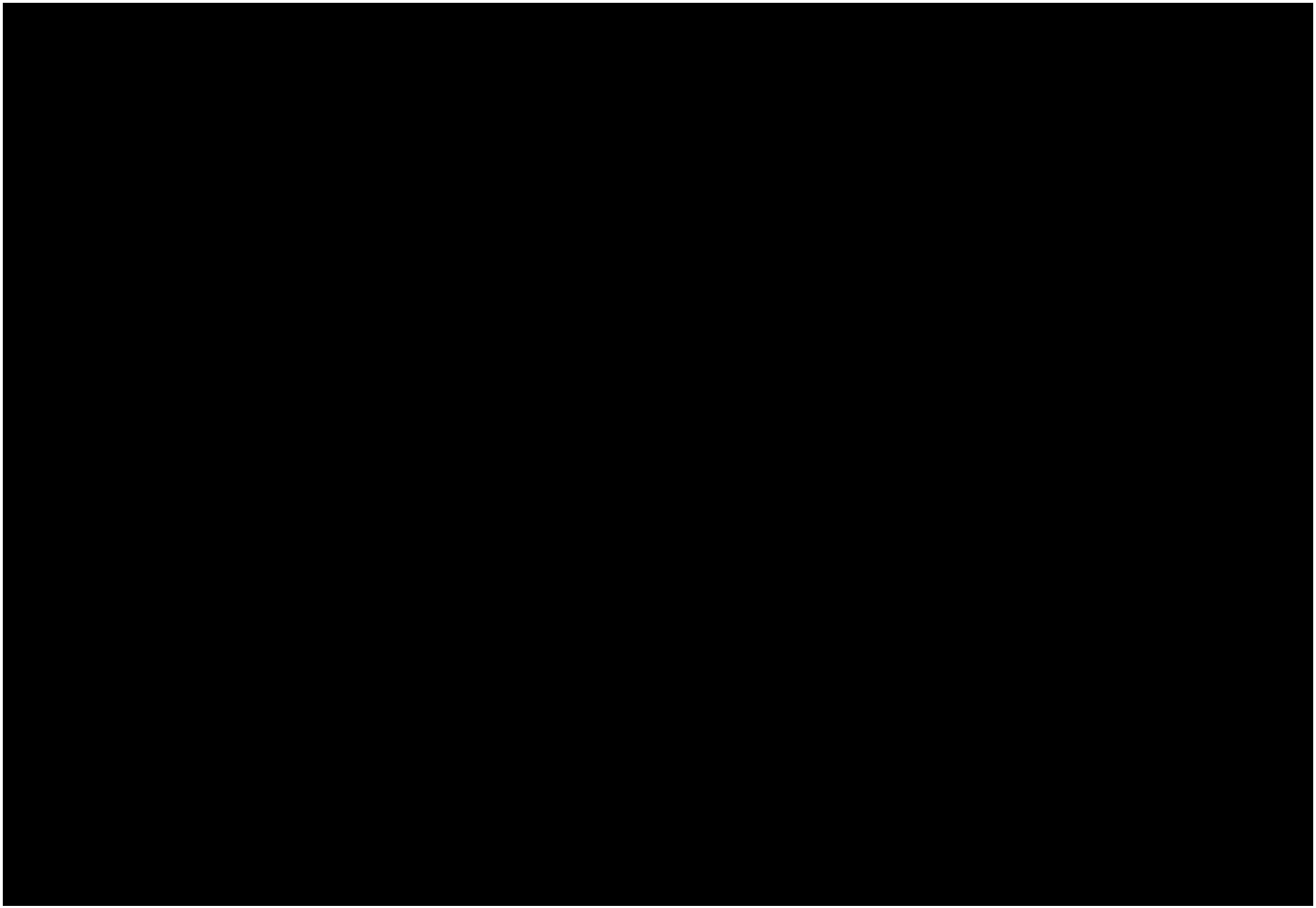


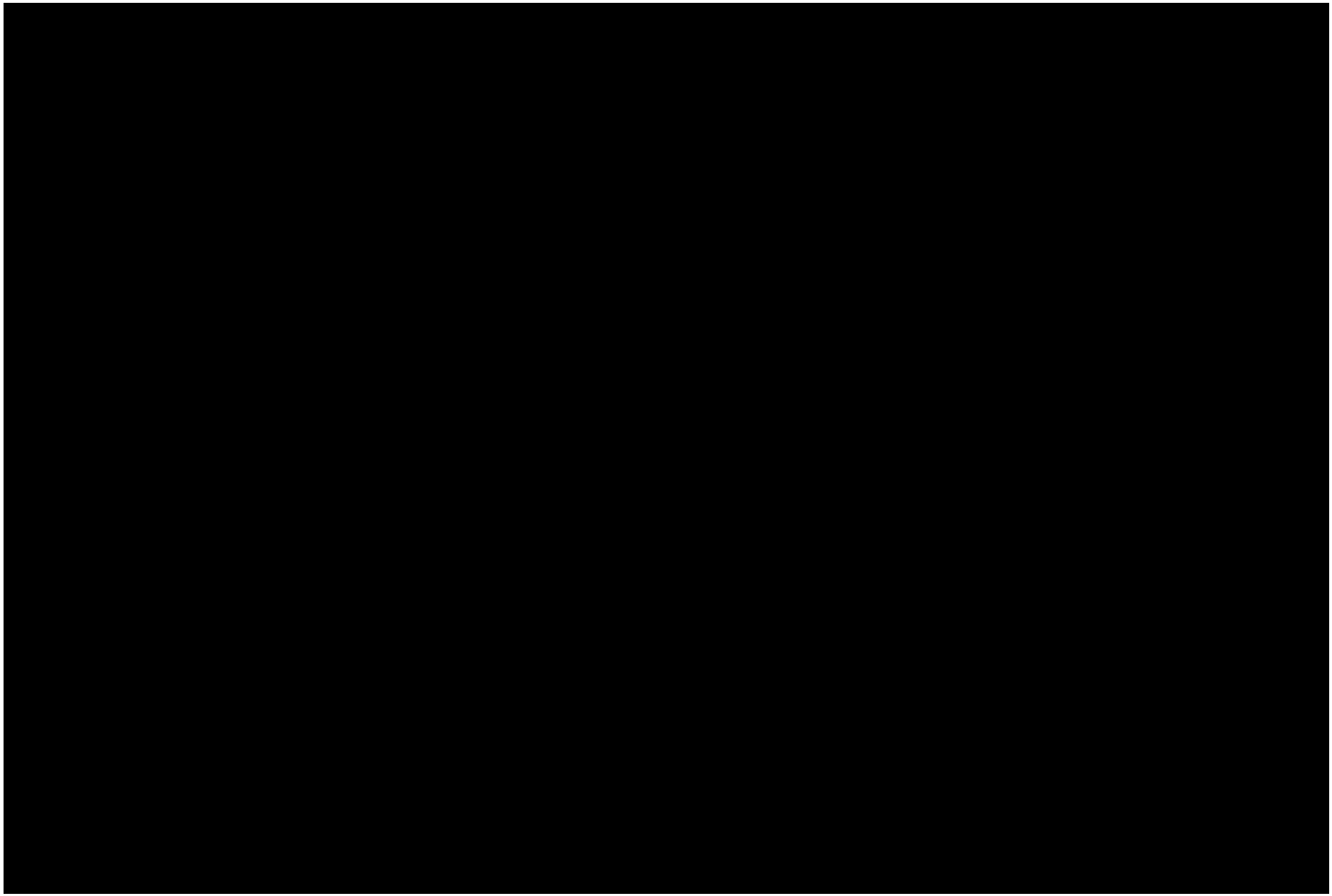


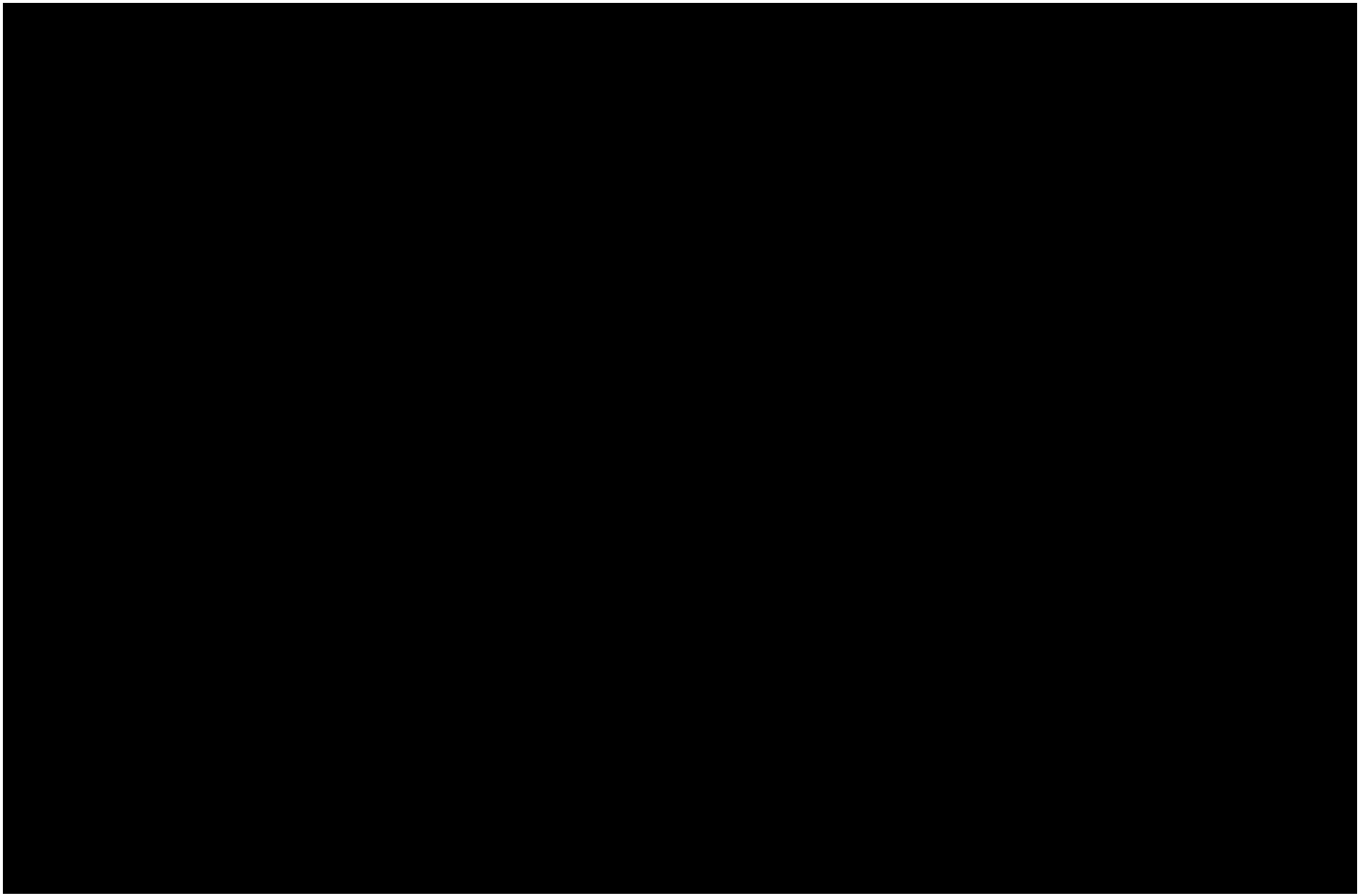


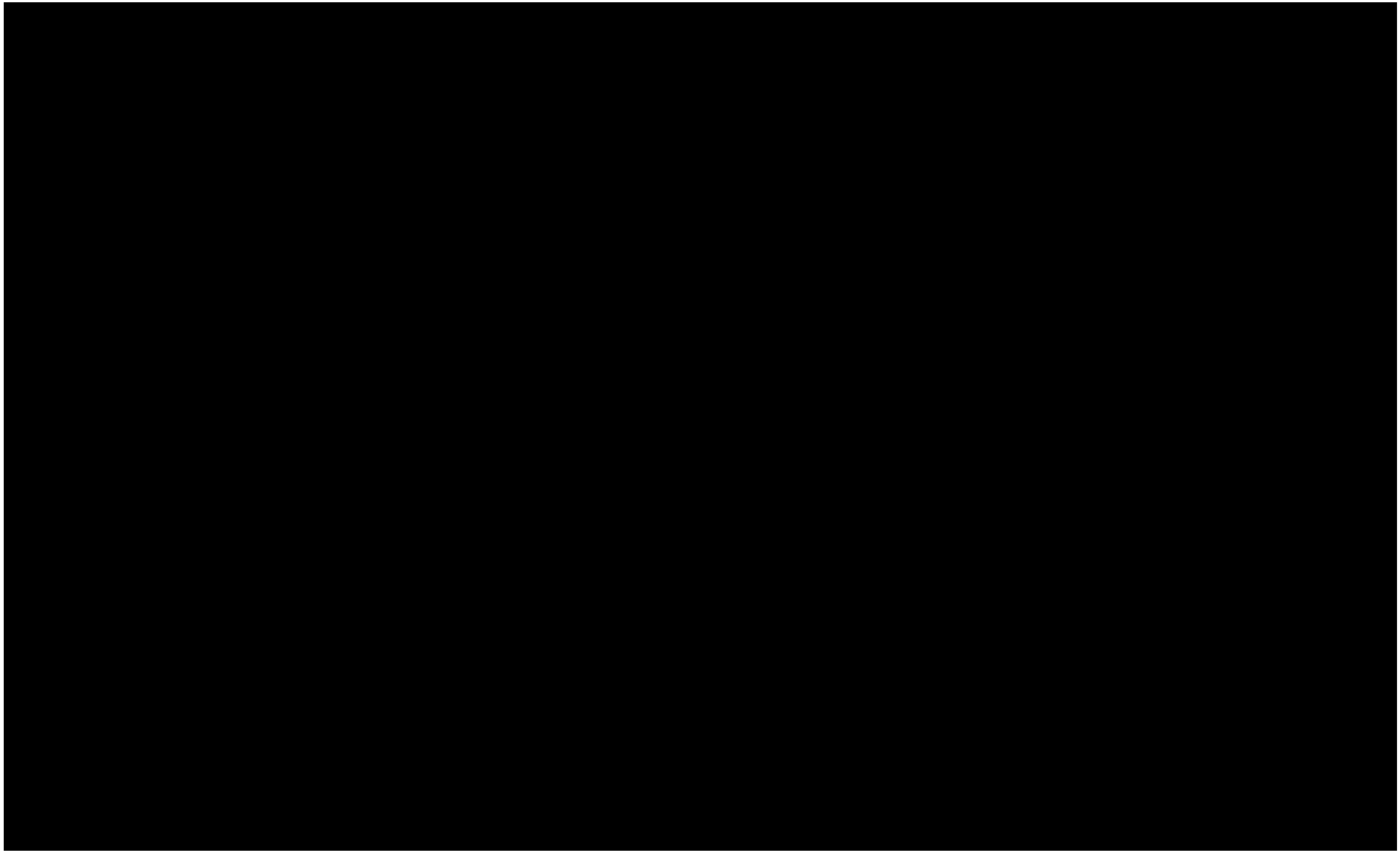


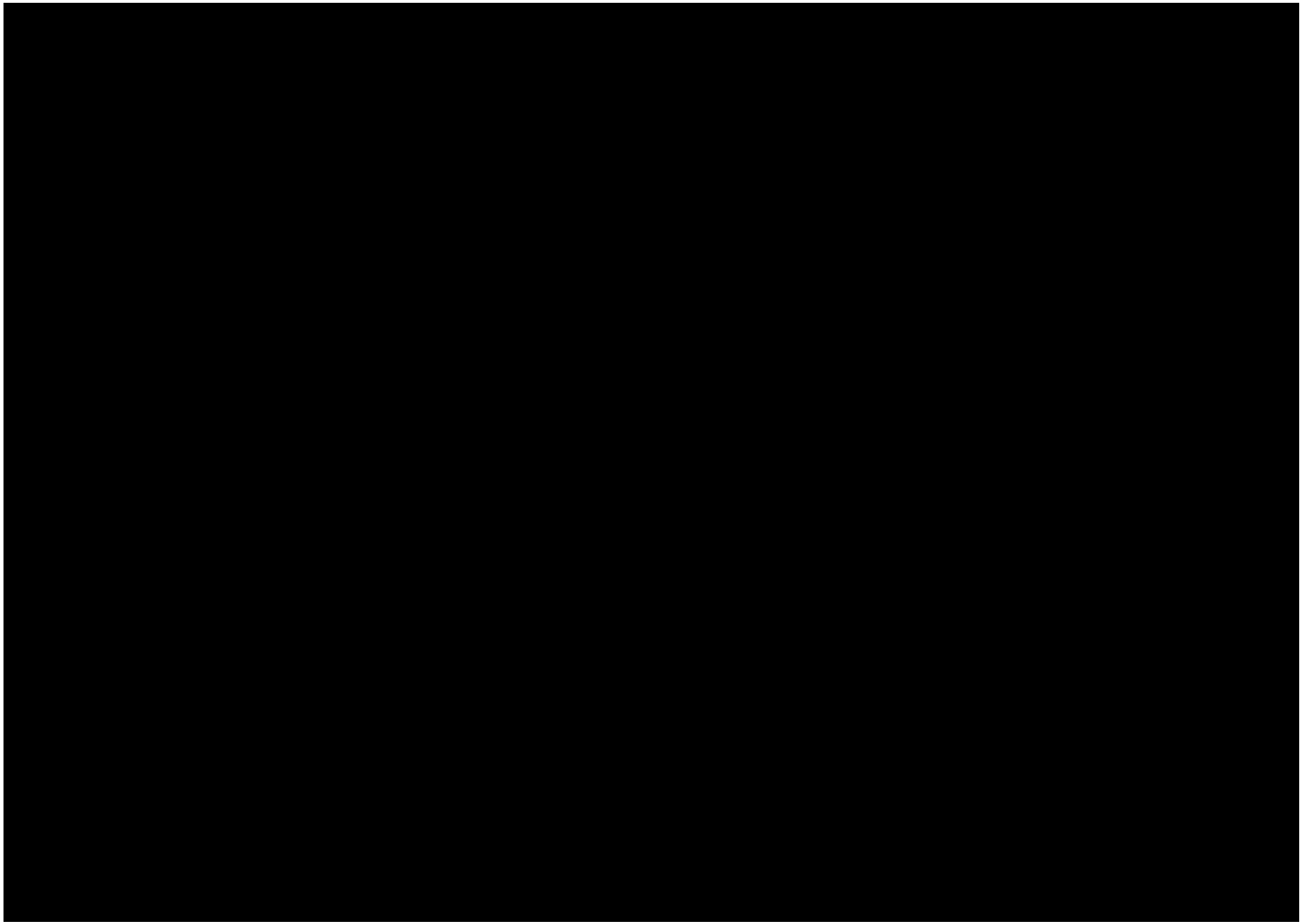


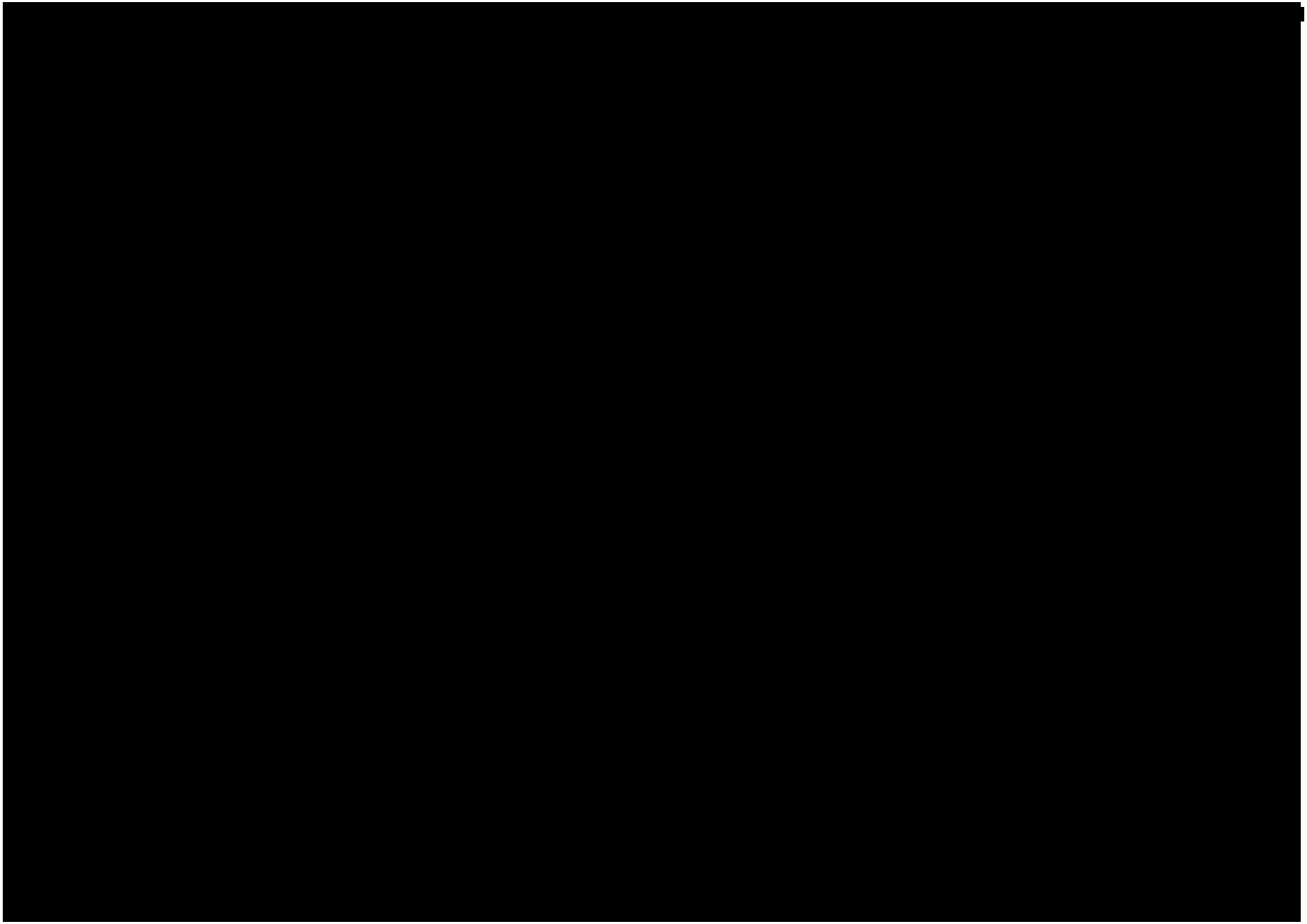


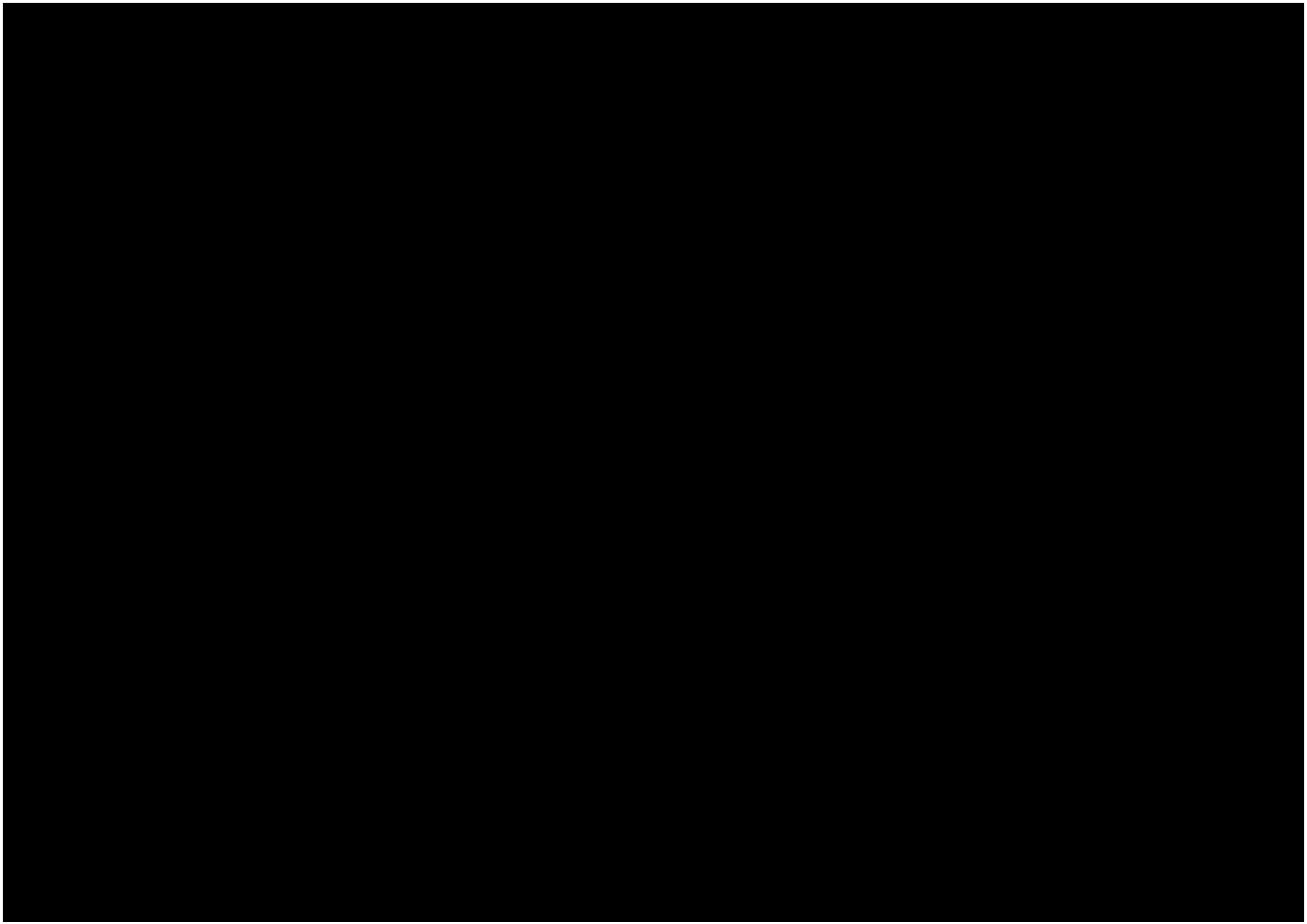


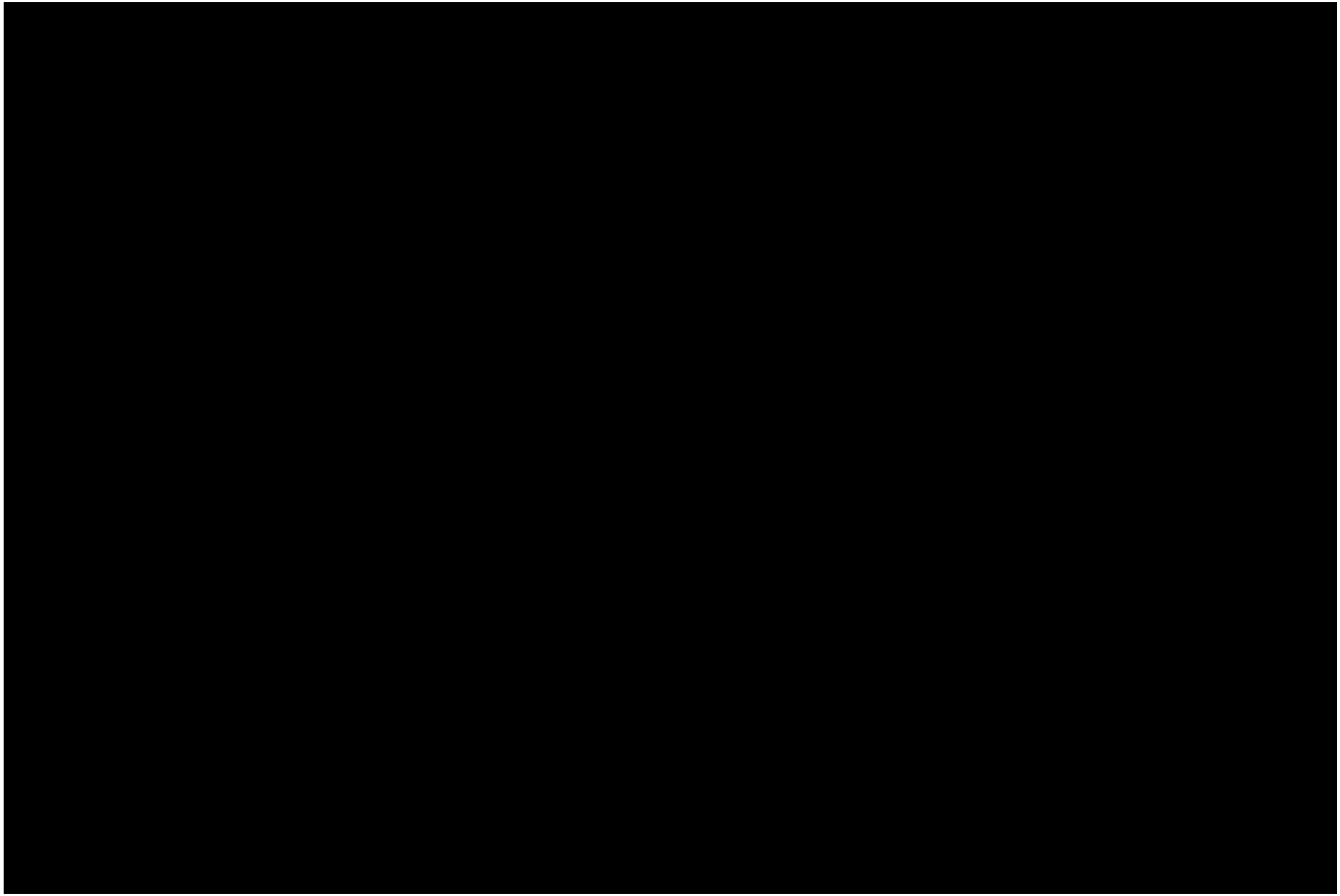


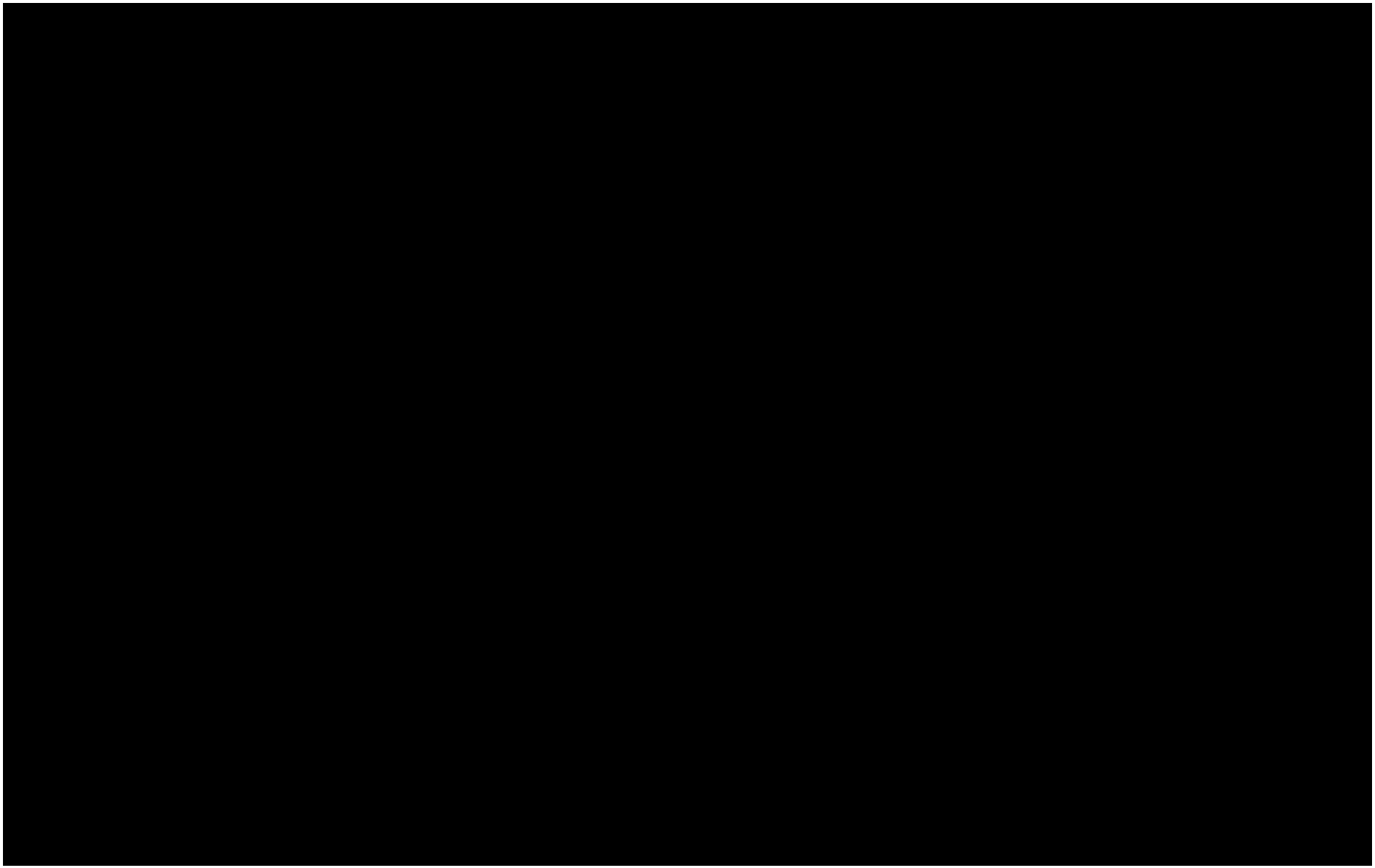


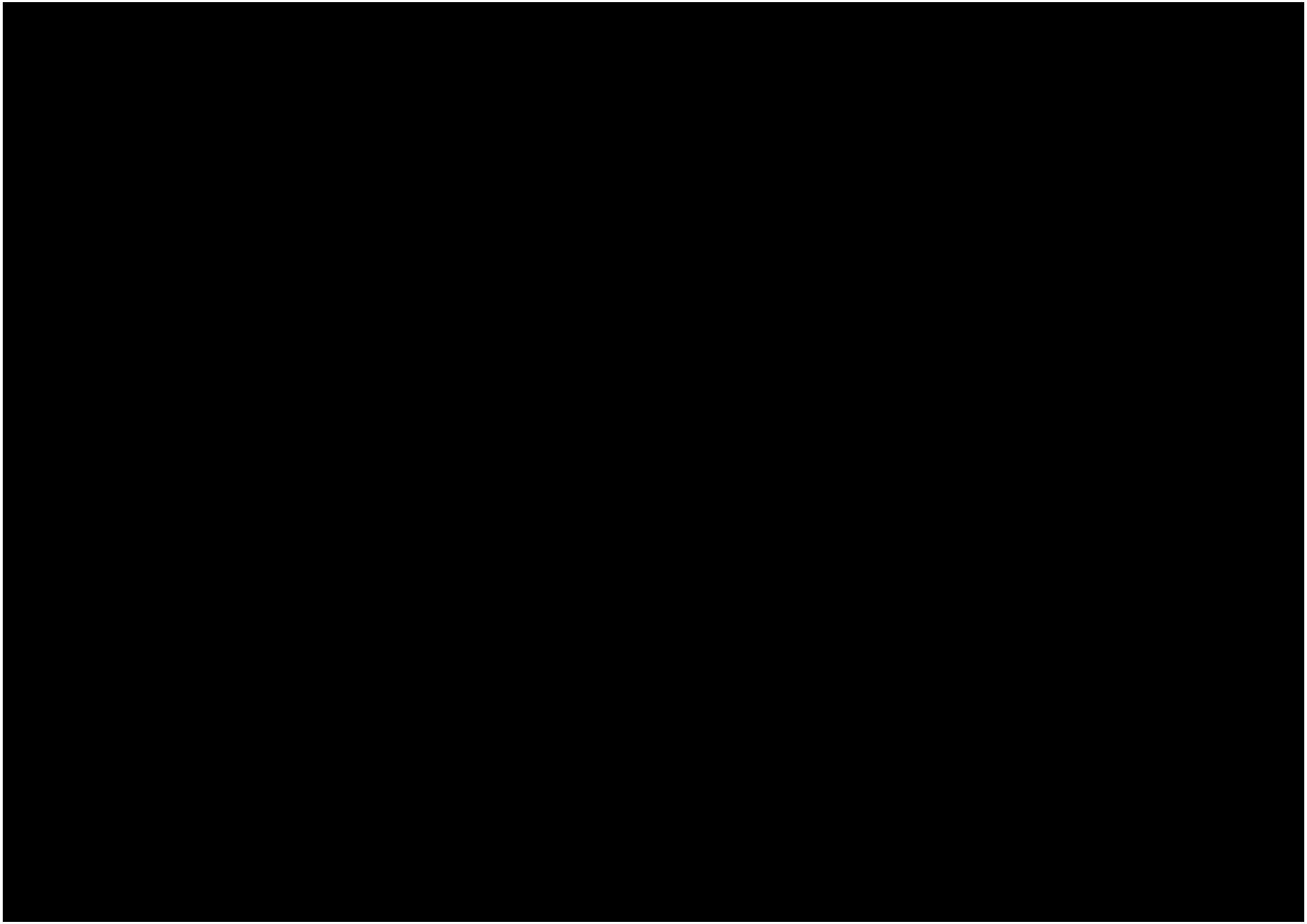


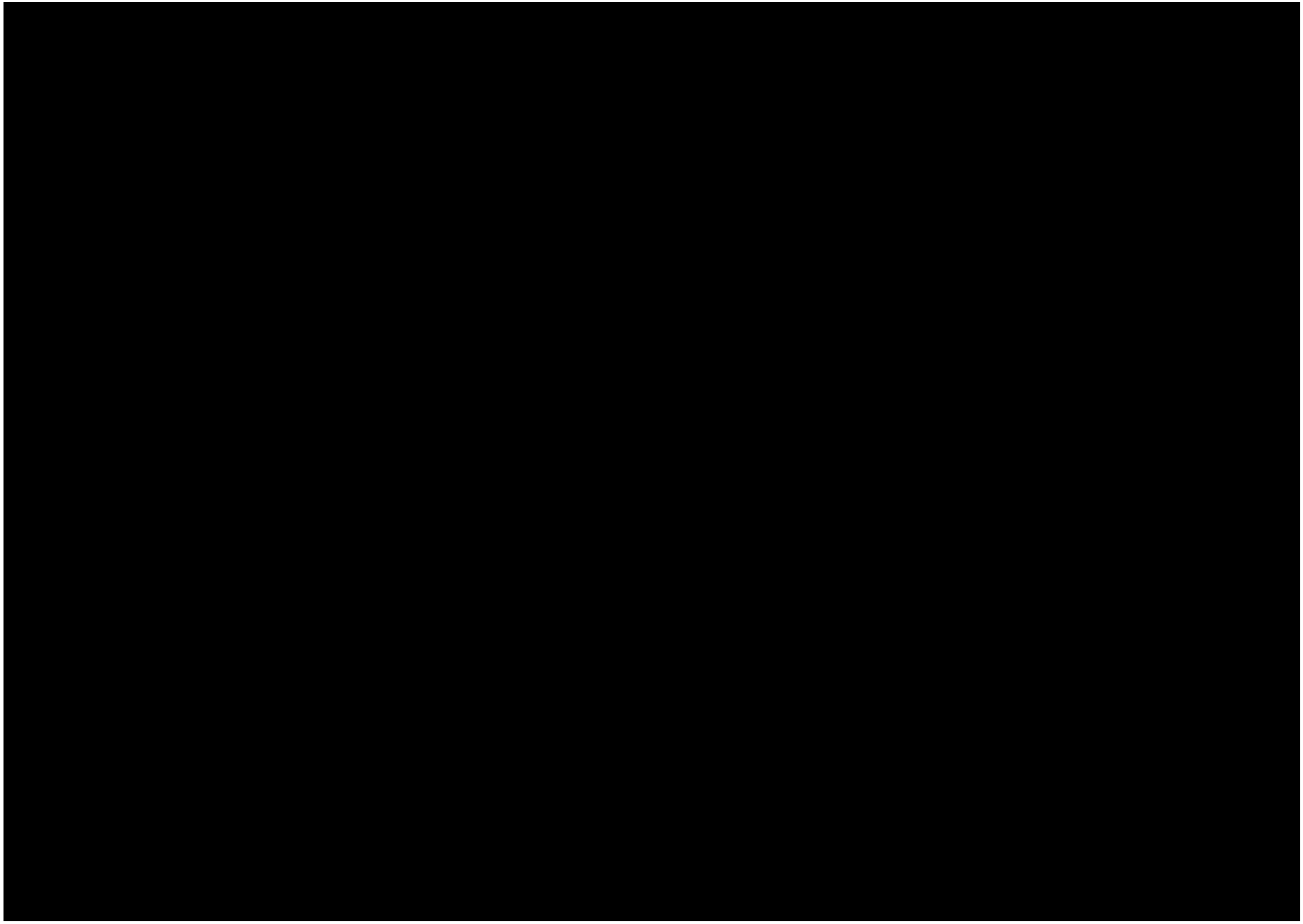


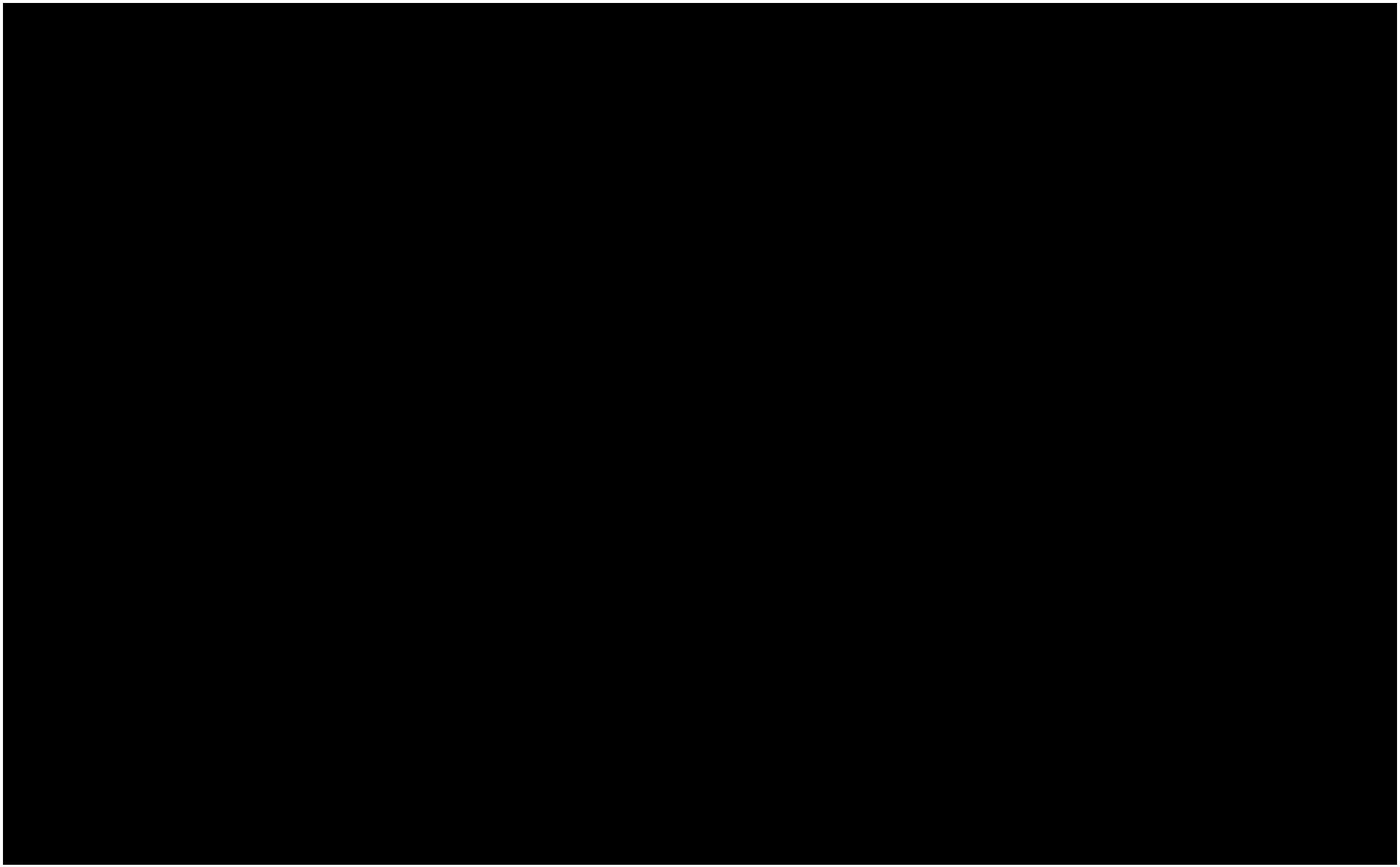


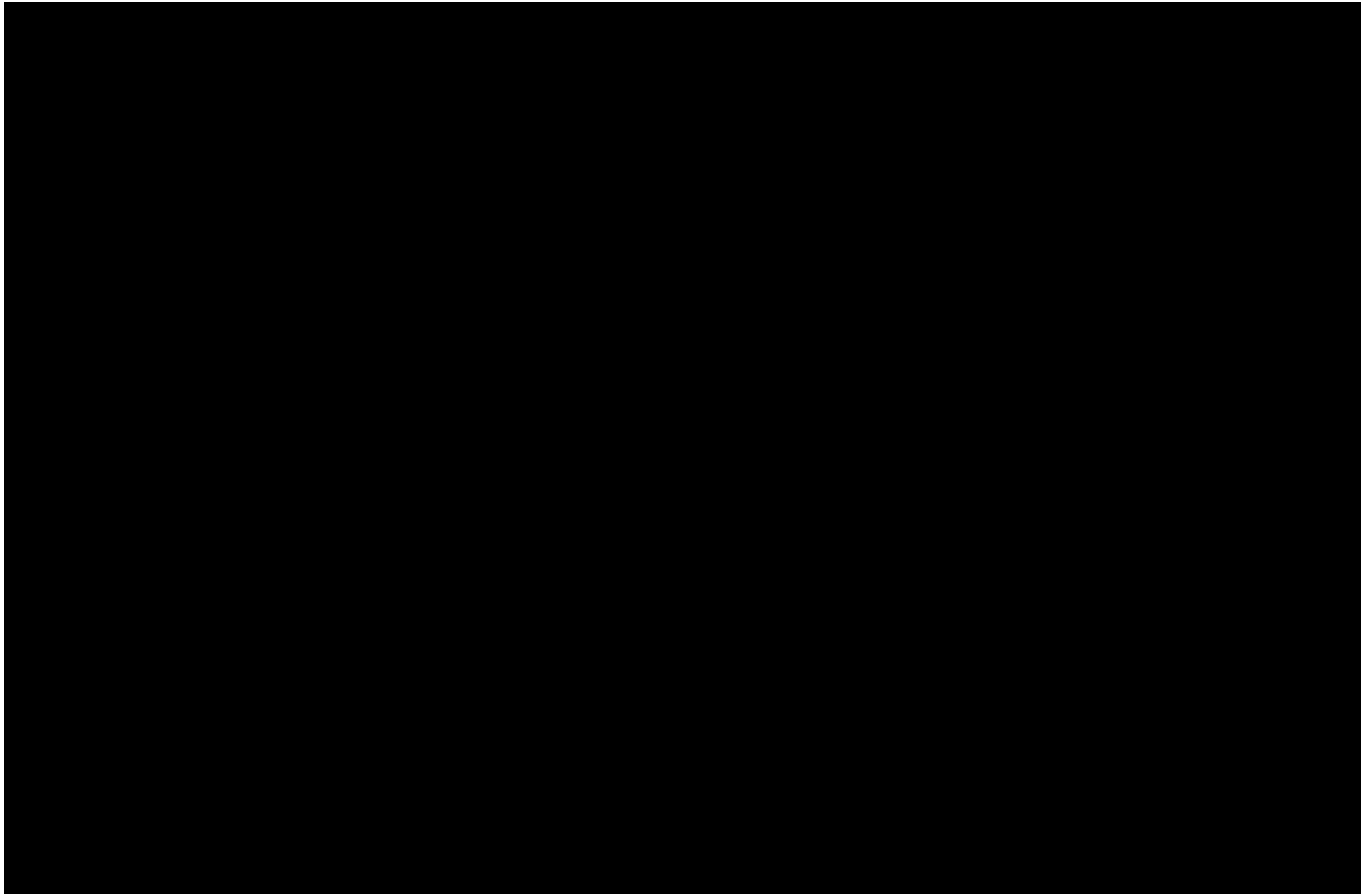












2. „Úpravy prostředí IP pro „obecná část aplikace“ pro práci s pacientem“

Předmětem rozšíření jsou nezbytné úpravy prostředí IP pro „obecná část aplikace“ pro práci s pacientem. Tato část obsahuje obecné položky a funkce použité ve všech budoucích kompozitních aplikacích. V rámci modulu pro kompozitní aplikace bude realizováno napojení na standartní služby komponent MPI, EHR a Auditního logování integrační platformy pomocí IHE profilů, kde bude možné a pomocí proprietárního rozhraní pro doplnění workflow.

Systém umožní vybírat pacienty z centrálního registru, evidovat pacienty, kteří v registru nejsou k nalezení. Pomocí komunikace s centrálním uložištěm dokumentů zobrazovat aktuální hospitalizace pacientů a k jednotlivým hospitalizacím evidovat pacientskou dokumentaci, které nejsou součástí této nabídky. Veškeré dokumenty budou evidovány na úrovni modulu s vazbou na generátor 1D a 2D kódů a následně odesílány do centrálního registru a repositáře dokumentů.

2.1. Obecná část aplikace pro práci s pacientem

Tato část obsahuje obecné položky a funkce použité ve všech budoucích aplikacích.