Order Form

In this Order Form, capitalised expressions shall have the meanings set out in Call Off Schedule 1 (Definitions), Framework Schedule 1 or the relevant Call Off Schedule in which that capitalised expression appears.

The Supplier shall provide the Services specified in this Order Form to the Customer on and subject to the terms of the Call Off Contract for the duration of the Call Off Period.

This Order Form should be used by Customers ordering Services under the Technology Services 2 Framework Agreement ref. RM3804 in accordance with the provisions of Framework Schedule 5.

The Call Off Terms, referred to throughout this document, are available from the Crown Commercial Service website http://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3804

The Customer must provide a draft Order Form as part of the Further Competition Procedure.

Section A
General information

This Order Form is issued in accordance with the provisions of the Technology Services 2 Framework Agreement RM3804.

Customer details
Customer organisation name Food Standards Agency
Billing address Your organisation's billing address - please ensure you include a postcode Clive House, 70 Petty France, Westminster, SW1H 9EX
Customer representative name The name of your point of contact for this Order [redacted]
Customer representative contact details Email and telephone contact details for the Customer's representative [redacted]

Supplier details
Supplier name The Supplier organisation name, as it appears in the Framework Agreement Methods Business & Digital Technology Limited
Supplier address Supplier's registered address Saffron House, 6-10 Kirby Street, London, EC1N 8TS

Supplier representative name
The name of the Supplier point of contact for this Order
[redacted]

Supplier representative contact details
Email and telephone contact details of the supplier's representative
[redacted]

Order reference number or the Supplier's Catalogue Service Offer Reference Number
A unique number provided by the supplier at the time of the Further Competition Procedure
Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management. If a Direct Award, please refer to the Supplier's Catalogue Service Offer Reference Number

N/A

Section B
Overview of the requirement

Framework Lot under which this Order is being placed
Tick one box below as applicable (unless a cross-Lot Further Competition)

1. TECHNOLOGY STRATEGY & SERVICES DESIGN ☐
2. TRANSITION & TRANSFORMATION ☐
3. OPERATIONAL SERVICES

a: End User Services ☐

b: Operational Management ☐

c: Technical Management ☐

d: Application and Data Management ☒

4. PROGRAMMES & LARGE PROJECTS

a. OFFICIAL ☐

a. SECRET (& above) ☐

Customer project reference
Please provide the customer project reference number.

FS430635

Call Off Commencement Date

The date on which the Call Off Contract is formed – this should be the date of the last signature on Section E of this Order Form

02/07/2021

Call Off Contract Period (Term)
A period which does not exceed the maximum durations specified per Lot below:

Lot	Maximum Initial Term – Months (Years)	Extension Options – Months (Years)	Maximum permissible overall duration – Years (composition)
1	24 (2)	-	2
2	36 (3)	-	3
3	60 (5)	-	5
4	60 (5) *	12 + 12 = 24 (1 + 1 = 2)	7 (5+1+1) *

* *There is a minimum 5 year term for this Lot*

Call Off Initial Period Months
24 months

Call Off Extension Period (Optional) Months
3 X 12 month extension periods (36 months total)

Minimum Notice Period for exercise of Termination Without Cause 90 days
(Calendar days) *Insert right (see Call Off Clause 30.7)*

Additional specific standards or compliance requirements
Include any conformance or compliance requirements over and above the Standards (including those listed at paragraph 2.3 of Framework Schedule 2) which the Services must meet.

No Additional standards Applicable.

Customer's ICT and Security Policy
FS430635_006 FSA Acceptance Into Service Procedure
FS430635_007 FSA Change Management Procedure
FS430635_008 FSA Incident Management Procedure
FS430635_009 FSA Security Incident Procedure 2019
FS430635_010 FSA Problem Management Process
FS430635_011 FSA Knowledge Management Procedure
FS430635_012 FSA Service Asset & Configuration Management (SACM) Procedures FS430635_013 FSA Supplier Access Policy August 2019 v1
FS430635_014 Service Capability High Level Principles
FS430635_015 FSA IT Acceptable User Policy
FS430635_018 FSA Request Fulfilment

Security Management Plan
The Supplier will create an information Security Management Document Set to document how they will comply with the specific FSA security requirements to be approved by the Head of Security at the FSA. This will be completed as part of On-boarding the supplier before the service begins.

Section C
Customer Core Services Requirements

Please provide details of all Services required including the locations where the Supplier is required to provide the Services Ordered.

Services
List below or append as a clearly marked document to confirm the Services which the Supplier shall provide to the Customer (which could include the Customer's requirement and the Supplier's response to the Further Competition Procedure). If a Direct Award, please append the Supplier's Catalogue Service Offer.

Please see Annex A for the Specification of Requirements, the Suppliers responses to the ITT and any post tender Clarifications. This make up the services to be carried out under this contract.

On occasion the FSA may require the supplier to engage on project work as part of this service, but not covered by the monthly service charge. This shall be commissioned using the work package template found under Annex B.

The contract includes a full copy of the ITT response forms submitted by Methods and CoreAzure (including Operational, Service, Transformational and Commercial requirements). Collectively they form a useful record of how the Supplier has proposed to address the ITT requirements set out in the Business Requirements Section of the FSA Cloud Infrastructure Management Requirements Specification document version 2 (Reference: FS430635_001).

It should be noted however, that there are questions included within the ITT that do not relate to baseline contractual requirements and, to be properly fulfilled by the supplier, may either need to be resourced from the project allocation (or subject to change control), or to be completed have dependencies that are beyond the control of supplier. As such, not all of the statements covering service descriptions and commitments contained within the ITT response reflect a contractual commitment by the supplier. All statements regarding the supplier's capabilities within the ITT are an accurate reflection regardless of baseline or extended scope and/or project dependencies. The Supplier's commercial response to Section 6B contains details of the baseline and capped services that are within scope of this agreement.

Location/Site(s) for provision of the Services

This service will be delivered remotely by the Supplier, with the occasional requirement to visit FSA Offices/Sites.

Additional Clauses *(see Annex 3 of Framework Schedule 4)*
This Annex can be found on the RM3804 CCS webpage. The document is titled RM3804 Alternative and additional t&c's v4.
Those Additional Clauses selected below shall be incorporated into this Call Off Contract

Applicable Call Off Contract Terms		**Optional Clauses** *Can be selected to apply to any Order*	
Additional Clauses and Schedules			
Tick any applicable boxes below		*Tick any applicable boxes below*	
A: SERVICES – Mandatory **The following clauses will automatically apply where Lot 3 services are provided (this includes Lot 4a & 4b where Lot 3 services are included).**	☒	C: Call Off Guarantee	☐
		D: Relevant Convictions	☐
A3: Staff Transfer		E: Security Requirements	☒
A4: Exit Management			
A: PROJECTS - Optional		F: Collaboration Agreement Where required please complete and append to this Order Form as a clearly marked document (see Call Off Schedule F)	☐
A1: Testing	☐		
A2: Key Personnel	☒	G: Security Measures	☐
B: SERVICES - Optional *Only applies to Lots 3 and 4a and 4b*			
		H: MOD Additional Clauses	☐
B1: Business Continuity and Disaster Recovery	☒		
B2: Continuous Improvement & Benchmarking	☒	**Alternative Clauses**	
B3: Supplier Equipment	☐	*To replace default English & Welsh Law, Crown Body and FOIA subject base Call Off Clauses*	
B4: Maintenance of the ICT Environment	☒	*Tick any applicable boxes below*	

B5: Supplier Request for Increase of the Call Off Contract Charges	☐	Scots Law Or	☐
B6: Indexation	☐	Northern Ireland Law	☐
B7: Additional Performance Monitoring Requirements	☐	Non-Crown Bodies	☐
		Non-FOIA Public Bodies	☐

Collaboration Agreement *(see Call Off Schedule F) This Schedule can be found on the RM3804 CCS webpage. The document is titled RM3804 Collaboration agreement call off schedule F v1.*

Not Applicable.

Licensed Software **Where Software owned by a party other than the Customer is used in the delivery of the Services list product details under each relevant heading below**

Not Applicable

Customer Property *(see Call Off Clause 21)*
Items licensed by the Customer to the Supplier (including any Customer Software, Customer Assets, Customer System, Customer Background IPR and Customer Data)
ServiceNow Licenses.
Any Devices Shared with the supplier to enable them to carry out aspects of the contract.
Microsoft Azure Licenses and permissions

Call Off Contract Charges and Payment Profile *(see Call Off Schedule 2)*
Include Charges payable by the Customer to the Supplier (including any applicable Milestone Payments and/or discount(s), but excluding VAT) and payment terms/profile including method of payment (e.g. Government Procurement Card (GPC) or BACS)

Initial Monthly charge for this service will be £33,132.50 based on the Initial Fixed Monthly charge Commercial Template attached.

[redacted]

Payments will be made by BACS, monthly in arears. Invoices will be submitted to [redacted] with a copy sent to [redacted]. All invoices must contain a Valid PO number and reference FS430635.

Undisputed Sums Limit (£) *Insert right (see Call Off Clause 31.1.1)*	£33,132.50

Delay Period Limit (calendar days) *Insert right (see Call Off Clause 5.4.1(b)(ii))*	NA
Estimated Year 1 Call Off Contract Charges (£) For Call Off Contract Periods of over 12 Months	Approximately £400,000, based on Monthly service charge.

Enhanced Insurance Cover
Where a specific Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Schedule 14 please specify below

No Enhanced Insurance cover required

Transparency Reports *(see Call Off Schedule 6)*
To be agreed between FSA and Methods during On-Boarding of the service.

Quality Plans *(see Call Off Clause 7.2)*

Time frame for delivery of draft Quality Plans from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) *Where applicable insert right*	To be agreed between FSA and Methods during On-boarding of the service.

Implementation Plan *(see Call Off Clause 5.1.1)*

Time frame for delivery of a draft Implementation Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) *Where applicable insert right. If a Direct Award, please append the Implementation Plan attached to the Supplier's Catalogue Service Offer.*	To be agreed between FSA and Methods during On-boarding of the service.

BCDR *(see Call Off Schedule B1)*
This can be found on the CCS RM3804 webpage. The document is titled RM3804 Alternative and additional t&c's v4.

Time frame for delivery of a BCDR Plan from the Supplier to the Customer – from the Call Off Commencement Date (Working Days) *Where applicable insert right*	45 days.

Disaster Period (calendar days)
Services with availability SLAs for 24/7/365 = 1 working day
All other services = 2 working days.

GDPR (see Call Off Clause 23.6)
Please see Schedule 7 appended to this Order form.

Supplier Equipment *(see Call Off Clause B3)*
This can be found on the RM3804 CCS webpage. The document is titled RM3804 Alternative and additional t&c's v4.
NA

Key Personnel & Customer Responsibilities *(see Call Off Clause A2)*
List below or append as a clearly marked document to include Key Roles

Key Personnel *List below or append as a clearly marked document to include Key Roles*	**Customer Responsibilities** *List below or append as a clearly marked document*
Head of Managed Service: [redacted] Client Representative: [redacted]	Click here to enter text.

Relevant Conviction(s)

Where applicable the Customer to include details of Conviction(s) it considers relevant to the nature of the Services.

List below or append as a clearly marked document (see Call Off Clause D where used)

Not Applicable

Appointment as Agent *(see Call Off Clause 19.5.4)*

Insert details below or append as a clearly marked document

NA

SERVICE LEVELS AND SERVICE CREDITS *(see Part A of Call Off Schedule 3)*

Service Levels

Introduction

Suppliers will be required to provide the Incident Management element of this agreement using the following parameters:

- Core or 'working' hours 7:00am to 8:00pm Monday to Friday
- Non-core 8:01pm to 6:59am Monday to Friday plus weekends and bank holidays

There will be no Service Credit/Debit regime associated with this call-off. Instead the target achievement levels detailed in Table A will attract failure points where resolution targets are not met. Performance against SLAs must be monitored and reported on by the Supplier. The Supplier must also identify why they have not been achieved and what plans are being instigated to ensure that this does not continue.

Incident Management

The following are the minimum performance levels that the Supplier should deliver to. The Supplier will be expected to report on these monthly and provide further details should one of these minimums not be achieved (i.e. attend Post Incident Reviews, provide Root Cause, Resolution, Avoidance and Remediation….):

Standard Incident Management Responsibilities for all suppliers include:

- Raising and maintaining incidents
- Triaging and prioritising incidents
- Providing regular and comprehensive updates
- Ensuring 3rd parties are provided with necessary information to enable resolution of incidents

The Supplier will carry out all Incident Management duties in accordance with the FSA's documented Incident Management procedures.

In the event of a P1 or P2 Incident major incident processes will be invoked, Supplier shall conduct a formal Problem Management review, which shall include undertaking a root cause analysis ("RCA") to determine the underlying cause of the Incident and providing guidance to support any activity required to amend the underlying cause.

Allocation of Incident levels (P1 – P4) will be done using the following table:

Table A – Incident Severity

Severity	Description	Response Time	Resolution Time	Target to be achieved in month
P1	Severe business disruption: business unit or sub-unit unable to operate, critical components failed. Failure to meet technological minimums.	15 Minutes from identification of issue	4 hours	No more than 1 failure
P2	Major business disruption: critical user(s) or user group unable to operate, or business unit experiencing significant reduction in system performance.	1 hour from identification of issues	8 hours for critical services, 8 working hours for non-critical services	No more than 1 failure
P3	Minor business disruption: single user unable to operate with no circumvention available	0.5 working day from identification of issue	3 working days	Either 90% or above OR no more than 2 failures
P4	Minor disruption: single user or user group experiencing problems, but with circumvention available	1 working day from identification of issue	3 working days	

*The Resolution Time starts when the incident is raised in Service Now and ends when the Incident is Resolved.

Adherence to incident management responsibilities will also be assessed via reviews of completed incidents.

Request Management

The following are the minimum performance levels that the Supplier should deliver to. The Supplier will be expected to report on these monthly and provide further details should one of these minimums not be achieved

Standard Request Management Responsibilities for all suppliers include:

- Carrying out request tasks within the allocated timescales
- Providing regular and comprehensive updates

The Supplier will carry out all Request Management duties in accordance with the FSA's documented Request Management procedures.

Description	Resolution Time	Target to be achieved in month
VM provisioning: establish a virtual server in the production, development, and test environment for all architectures, and operating systems supported by the environment. This must include all necessary updated documentation and configuration within FSAs management systems	1 working days	No more than 1 failure
VM decommissioning: decommission a virtual server from the production, development, and test environments. This must include all necessary updated documentation and configuration within FSAs management systems	1 working day offline, 5 day warranty	No more than 1 failure

Infrastructure management

The following are the minimum performance levels that the Supplier should deliver to. The Supplier will be expected to report on these monthly and provide further details should one of these minimums not be achieved

Description	Target to be achieved in month
Operational availability of / connectivity to Virtual servers / services	99.5%
Ensure that virtual servers are patched in accordance with the agreed patching schedules (including restart) and operating systems are updated and maintained at versions in mainstream support.	100%

Additional KPIs

The Supplier will be required to demonstrate, monthly, that they are meeting the following KPIs (via suitable management information):

- Performance reporting and analysis interfaces between Azure and Office 365 services, to be provided on a monthly basis.
- Performance management of the servers – Reporting of basic server performance, to enable the owners of services running on the machines to make decisions about performance. All statistics should cover peak and average figures, and should be incorporated into trend analysis
    - CPU utilization
    - Memory used
    - Network utilization – in and out
    - Disk performance and volumes – read and write operations
    - Disk utilisation

- RCA within 3 working days for P1 and P2 incidents
- Report on failed changes or changes causing issues with reasons

Notes

As new technologies are introduced / transitioned to, the FSA reserve the right to introduce new SLAs to reflect these. New SLA's will be mutually agreed between the FSA and the supplier prior to their introduction.

Additional Performance Monitoring Requirements
Technical Board – Not Applicable

Section D
Supplier response

Suppliers - use this section to provide any details that may be relevant in the fulfilment of the Customer Order

Commercially Sensitive information
Any information that the Supplier considers sensitive for the duration of an awarded Call Off Contract
Click here to enter text.

Total contract value
Please provide the total contract value (for the Call Off Initial Period) as detailed in your response to the Customer's statement of requirements. If a Direct Award, please refer to the Price Card as attached to the Supplier's Catalogue Service Offer.
The Contract Value is capped at £1,100,000 for the initial contract term, covering the Monthly Service Charge and capacity for contract related project work. The FSA and Methods will agree additional capacity as part of any variations to extend this agreement.

Section E
Call Off Contract award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 2 Framework Agreement RM3804.

The Supplier shall provide the Services specified in this Order Form to the Customer on and subject to the terms of this Order Form and the Call Off Terms (together referred to as "the Call Off Contract") for the duration of the Call Off Contract Period.

SIGNATURES

For and on behalf of the Supplier

[redacted]	

For and on behalf of the Customer

[redacted]	

CALL OFF SCHEDULE 7: SCHEDULE OF PROCESSING, PERSONAL DATA AND DATA SUBJECTS

Description	Details
Subject matter of the processing	There is no foreseen requirement of processing personal data under this contract, however the supplier will have access to personal data captured in ServiceNow. As this contract is for the management of the FSA's Cloud Infrastructure it may be that the supplier is required to investigate incidents such as security incidents that will include processing personal data for example reviewing logs. There may also be processing of personal data associated with the service of providing backups.
Duration of the processing	Processing will take place over the duration of the contract. This is due to expire on the 01/07/2023 with an opportunity to extend by up to another 3 years (+1 +1+1).
Nature and purposes of the processing	Personal and staff data is captured and stored in the FSA's ServiceNow for the purpose of facilitating IT support and Management in the FSA. It is used to log and track problems / incidents, as well as requests for staff equipment and specialist software. The supplier will not be required to contact the person directly as this is managed by the FSA's Service Desk supplier. All data is stored in the FSA's own ServiceNow Instance, and no processing of personal data will take place outside of this, meaning there is no destruction of data required upon the end of this contract. The supplier will be required to operate projects on behalf of the Agency. Should personal data be accessed it will be done so via FSA's infrastructure. This will mean the supplier will have access to the names and email addresses of FSA staff and other suppliers.
Type of Personal Data	Name, home address, personal phone numbers Staff data stored includes Name, Job Title, Department, staff Number, Grade, Work email and phone number, work location, Company and Manager. Other FSA supplier contact details such as name and email address and phone numbers.
Categories of Data Subject	Staff, contractors and suppliers.

Plan for return or destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	*N/A Data will not be retained by the supplier.*

Annex A – Specification of Requirements and Methods ITT response.

Statement of Requirements

Purpose

The purpose of this document is to detail the business requirements for the operation, support and continual improvement of our Cloud Infrastructure.
We are seeking to determine the optimum fashion for a phased transformation from our current model which comprises a significant proportion of managed hosted devices (IaaS) along with some platform (PaaS) and some software services (SaaS), to a future model which has a much greater degree of PaaS SaaS services.
A key element of the successful bid will be a compelling explanation of cost-effective sun-setting of the IaaS elements, and appropriate uplift in the PaaS and SaaS elements.
This explanation should include descriptions of how you would contribute to the assessment of the balance between PaaS and SaaS and how you will collaborate with the application lifecycle management provider to continuously and iteratively migrate to that future state.
Supporting the move to PaaS and SaaS is a requirement to work with the FSA's Technology, Digital and Data teams to support the underpinning tools for storage, management, analysis, integration, publication and protection of the organisation's data. This will include not just structured database management tools, but also EDRM systems, unstructured document and BLOB storage, business intelligence and analysis tools.
The contract holder will also be responsible for implementing, managing and routinely testing the FSA's backup, restore and Business Continuity Disaster Recovery strategy for our core IT services.
FSA operates in an environment where 24/7 management is necessary to ensure availability of services across the full extent of the FSA working day. We cannot rely on in-hours detection of service failures as this has a significant impact on FSA productivity.

Background

The Food Standards Agency is a non-ministerial government department of over 1300 people, with a big vision – to drive change in the food system so that it delivers "food we can trust". As the country has now transitions from the EU, the scale of this challenge cannot be underestimated. More than 90% of food and feed law in the UK currently comes from Europe and our primary goal is to continue to protect public health and UK consumers' wider interest in food.

The context in which we operate has transformed and continues to change at an unprecedented rate. Digital is the primary way we carry out our work, it is key to achieving our ambitions and transforming the way we do business and we continually strive to provide better online services to external stakeholders and internal customers to achieve faster and more effective models of delivery at optimal cost.

Our Digital services are supported by a number of specialist delivery partners providing Data Centre Hosting, End User Compute, Service Desk, Wide Area Network, LAN, Application Support, Telephony and Videoconferencing. At the heart of that arrangement is an internal team with the knowledge of our business, our systems and our obligations to enable them to integrate and manage the quality of our services. Key to the success of this multi-vendor model is Support Partner willingness and commitment to work in partnership, collaborating autonomously with other third-party suppliers within a culture of trust and shared goals.

The current disaggregated contract model has been in place since 2017 and as the composite contracts are approaching their maximum term, the FSA has taken the opportunity to review and reconfigure the structure of our contracts and ensure our specifications align with business needs. The output of this review can be found in the FSA's IT Roadmap document [See FSA30635_016 ODD IT Evergreen Technology Roadmap] which sets out our revised service groupings and our core principles for future digital service development, delivery and support.

Our goal is to be 'evergreen', perpetually updating and improving our services, continuing to adapt to business and political change and adopting new technologies as they emerge. We look to our support partners to be equally flexible and innovative in their approach to delivery, with a strong focus on continuous improvement and quality of service. One of the key benefits of a multi-vendor model is the opportunity to work with specialist suppliers, we want to be guided by expert advice and encourage our support partners to make recommendations based on their experience and a shared desire to improve and evolve.

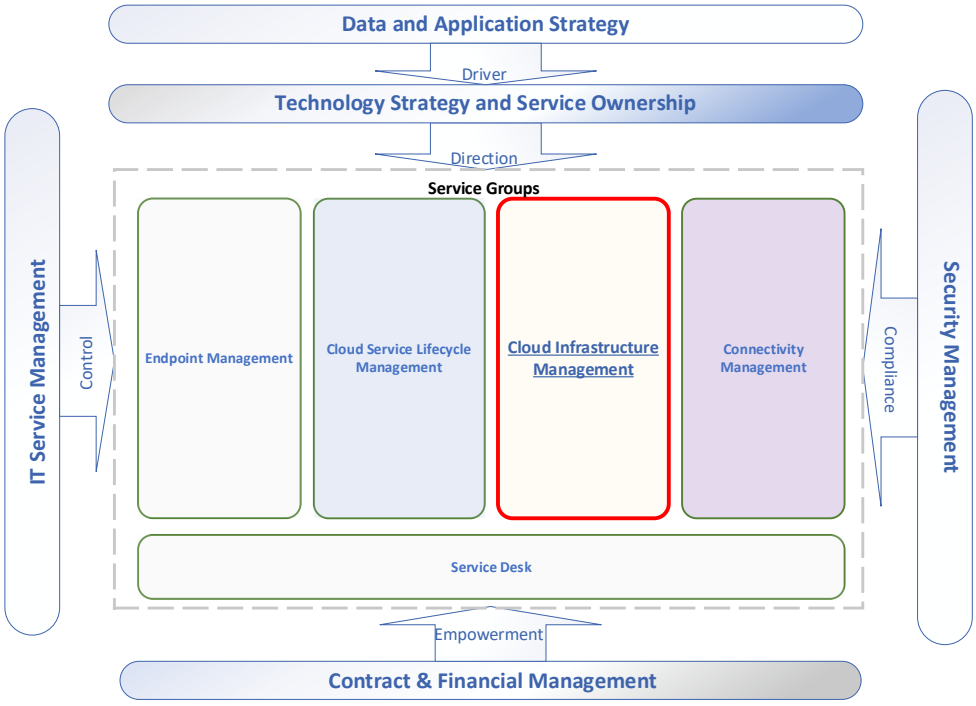
1.1 FSA Transparency

The Agency is committed to openness, transparency and equality of treatment to all support partners. As well as these principles, for science projects the final project report will be published on the Food Standards Agency website (www.food.gov.uk).

In line with the Government's Transparency Agenda which aims to encourage more open access to data held by government, the Agency is developing a policy on the release of underpinning data from all of its science- and evidence-gathering projects. Underpinning data should also be published in an open, accessible, and re-usable format, such that the data can be made available to future researchers and the maximum benefit is derived from it. The Agency has established the key principles for release of underpinning data that will be applied to all new science- and evidence-gathering projects which we would expect support partners to comply with. These can be found at http://www.food.gov.uk/about-us/data-and-policies/underpinning-data.

General Specification

This group of services sits within the overall IT Governance architecture below:



Endpoint Management	**What do we provide?** Ensure that users of FSA IT are provided with the devices and endpoint software required to do their job and that this is properly secured, managed and when necessary replaced.

Cloud Service Lifecycle Management	**What do we use it to do?** Focusses on maintaining application spaces and containers, development tools, but the primary focus is on enabling FSA to make the best use of cloud service offerings and, in particular, to facilitate and implement application migration from server based IaaS to Platform and Software services.
Cloud Infrastructure Management	**Where do we keep it?** The maintenance and improvement of those data storage services. Management of the overall Azure tenant architecture, it's subscriptions, resource groups, service monitoring, security and reporting and enabling functionality to extend or be replicated across multi-cloud environments. There is also scope for additional AWS and Google hosted applications which will require host management, and potentially a need for further environments to meet specific business needs. Consequently, we are seeking a support partner who can manage hosting predominantly in a single environment, but with the expertise to accommodate others. Responsibility also sits here for maintaining the FSA's test and development environments
Connectivity Management	**How do we get to it?** FSA requirements have moved on from the traditional corporate LAN/WAN infrastructure to prioritise the ability to connect to Office 365, Azure and other Cloud Services from any location. This will potentially encompass a change from the current model which has responsibility for connectivity by the network management provided stopping at the "front door" of the hosting environment, to a model where all network management and configuration, including those elements within a cloud hosting environment, fall under the responsibility of the connectivity management provider.
Service Desk	**Who do I call when it breaks?** Service Desk is critical the day to day support for end users, but equally provides the toolset for capturing, storing and managing service information. This will continue, alongside a strategic aim to automate workflows and encourage increasing user self-service through a growing knowledge base and increased use of artificial intelligence tools in support of this

In 2017-18 we migrated our core technology infrastructure from on-premise data centres to Microsoft Azure, mainly as a Virtual Machine centred Infrastructure as a Service environment. Within that, we had a specific requirement to provide DBA support for several SQL Servers. The period since then has seen increased use of Azure services, particularly in the database area and this is a progression we're looking to build on significantly over the coming years.
We're looking for a support partner who will ensure that the cloud hosted environment is scaled appropriately, that services are available as required and are secure, accessible, backed up and that performance monitors, alerts and reports are manged effectively and integrated with our Service Management toolset (ServiceNow).
At the same time, this requirement is not purely for "as-is" operation and support. Our expectation is that many of the services FSA consumes will increasingly be able to be provided by standard (albeit specially configured) SaaS services. As such we will be looking for pro-active advice and initiative from a Subject Matter Expert partner, both in on-boarding new services and extending cloud architectures to encompass these. We will also be looking to decommission legacy and sunset infrastructure and our expectation is that the IaaS elements of our estate will diminish as PaaS and SaaS elements increase. Although Microsoft Azure will remain the hub of our cloud infrastructure, we anticipate that there will be requirements for services in other hosted spaces and this will need to be aligned and supported as well.
The contract holder will also be responsible for ensuring that our Cloud infrastructure is secure and will have the expertise and appetite to continuously improve security to keep pace with new approaches and respond to ever increasing and evolving cyber threats.

1.2 In Scope

1. Tenant Architecture
2. Backup, Business Continuity and Disaster Recovery
3. Data Storage Systems
4. Database Management
5. Service Monitoring, alerting and Reporting Tools
6. Certificate Management
7. Test and Development Environments
8. Access Controls
9. Log Stores and Analytics

1.3 Out of Scope

1. Active Directory	Although operation of access controls, service roles and services such as Privileged Identity Management sits within this service group, responsibility for overall support and operation of the FSA Active Directory lies with Cloud Service Lifecycle Management
2. Network Provision	Network provision – including the configuration of Azure Virtual Networks, VPNs and Express Routes and the networking elements of other cloud hosting platforms - will be delivered through the Connectivity workstream.
3. Application Migration	Cloud infrastructure Management will be responsible for providing and operating the infrastructure to support the migration of applications from IaaS to PaaS/SaaS services, but the actual migrations will be the responsibility of Cloud Service Lifecycle Management
4. Data Architecture	This is the responsibility of the FSA's Data Team

Commercial Approach

FSA completed Premarket engagement on 26th October 2020. If you were unable to attend the Supplier Engagement Meeting, the slides can be found attached to Bravo [FS430635_002 Request for Information FSA Cloud Infrastructure Management, FS430635_004 Cloud Infrastructure Management - Supplier Engagement Meeting]. During this meeting a number of questions were asked, these were recorded along with questions emailed in to ODD.Contracts@food.gov.uk. Answer to these questions can be found attached [FSA430635_005 Cloud Infrastructure Management Clarification Questions].

FSA are looking to award a contract term is for 2 years with 3 separate possible extensions (i.e. 2+1+1+1) subject to satisfactory performance. The maximum contract duration is 5 years.

As part of this tender process FSA will not publish finances relating to existing actuals of the incumbent supplier or approved budget for 21/22. FSA requirements the Support Partner to develop monthly costs as outline the Commercial requirements/questions.

Business Requirements

Overview

The FSA requires a support partner to provide management of its cloud infrastructure service, including the overall Azure tenant architecture, it's subscriptions, resource groups, service monitoring, security and reporting and enabling functionality to extend or be replicated across multi-cloud environments.

The support partner will need to work in a multi-supplier model, working in collaboration with other support partners and FSA teams. The FSA IT team will provide the overall management and strategy for both technical architecture and service management.
The support partner will work with the FSA service management team and other support partners to deliver value to customers, optimise efficiency and ensure continual improvement, working to ITIL principles and ensuring that their practices reflect all aspects of the ITIL service lifecycle.

Service Metrics

Please see FSA30635_017 FSAs Cloud Infrastructure Service Metrics for Service Metrics. Please use these metrics your financial response within our commercial requirements/questions area.

Operational Requirements

Service	Requirement	Priority
1. Tenant Architecture	• Deployment, support and operation of subscriptions, resource groups and workspaces • Support and optimisation of the Azure Infrastructure as a Service environment • Deployment, support and operation of Certificate services • Ensure that retained IaaS virtual servers are patched and operating systems are updated and maintained at versions in mainstream support.	Must

Service	Requirement	Priority
	• Service performance and accessibility must be optimised for use from multiple locations including remote and mobile users	
2. Database Management	• Deployment and operation of Microsoft and Postgres SQL databases using Database as a Service, Managed Instances and SQL Server • Deployment and operation of data repositories and analysis tools, including Azure Data Warehouse services	Must
3. Data Storage	• Deployment and operation of data storage in Azure, including BLOB storage and Data Lake services. • Support for Azure File storage and for legacy fileserver and document management storage pending their decommission. • Legacy Support should be assumed to include design, planning and delivery of content migration from file stores and servers and a legacy EDRM solution to manageable structures, e.g. SharePoint Online • Pro-active monitoring of all storage to ensure cost-effective utilisation	Must
4. Monitoring Tools/ Log Stores and Analytics	• Detect, respond to and fix anomalous patterns and service outages 24/7 with Root Cause Analysis taking place in line with the Problem Management Process • Provide and support mechanisms for ensuring such alerts/outages/anomalies are logged in FSA's ServiceNow instance and reported to the Service Desk • Use output of Root Cause Analysis to update knowledge management articles so that 1st line support can fix issues with increasing competence • Ensure that FSA receives both regular and exception reporting of the above and that FSA Technical and Service Management teams have access to required reports and dashboards.	Must
5. Back Up Restore and Disaster recovery	• Implement, operate and continually improve a unified backup strategy for the FSA's Azure environment, including all the above services, plus applications, virtual machines and other services. • Undertake regular testing and verification of both backup and restore processes to ensure that all data and service restoration from brick level to full datacentre recovery is fit for purpose • Work with FSA IT to ensure that backup capabilities and requirements are included in any service deployments outside the Azure tenant. • Implement, manage and continually improve the Business Continuity and Disaster Recovery strategy for FSA IT Services. - periodic testing and validation section on monitoring tools etc and regular improvement monitoring.	Must
6. Access Controls and Data Security	• Work with application support partners to ensure that O/S, Application and Database patching and version management is N-1 compliant • Management of Access Permissions and User Roles • Work with the FSA's Security and information management teams to ensure that all data storage and management systems are securely configured in line with NCSC guidance for Official/ Official-Sensitive • Ensure that GDPR and other relevant legislation is implemented and maintained effectively across the estate.	Must

Service	Requirement	Priority
	• Operate and act upon security management and monitoring tools, including the collection, storage and accessibility of log analytics. • Manage and provision spaces within hosted environments for public facing services, ensuring that these are effectively segregated	
7. Test and Development Environments	• Support, operate and continually improve the FSA's hosted Test and Development environments, ensuring effective segregation from the Production environment	Must
8. Certificate Management	• Support, operate and continually improve the FSA's certificate server infrastructure • Issue and update certificates for both internal and public facing services.	Must

Transformation Requirements

Service	Requirement	Priority
1. Tenant Architecture	• Where cloud hosting is required outside the FSA's Azure tenant, ensure that this is managed consistently and to the same standard as the above. • Provide expertise to inform FSA evaluations of multi-cloud hosting options, including pro-active advice on the infrastructure, security and support of adopting new services	Must
	• Enable and support the continual migration of applications from Infrastructure as a Service to Platform/ Software as a Service alternatives • Provide technical, support and contractual architectures to enable a decreasing requirement for Azure VMs and a corresponding upscale of other services.	
2. Data Storage	• Provide technical, support and contractual architectures to enable a decreasing requirement for SQL Server VMs and a corresponding upscale of other database services. • Ensure that data storage solutions have the flexible capacity to enable dynamic and cost efficient up and downscaling of storage capacity • Provision content driven hosting and storage solutions and enable the expansion of data warehousing, data science tools and non-relational storage.	Must
3. Monitoring Tools	• Enable increasingly proactive and Service Capacity, Availability and Performance Monitoring • Make innovative use of Artificial Intelligence and Machine Learning for operational management and work with FSA to deliver service efficiencies through use of AI	Should

4. Test and Development	• Implement and operate process for the rapid provisioning and deprovisioning of resources in the Test and Development environments. • Facilitate user and developer self-service within these environments, while continuing to protect the production environment against unauthorised change or services becoming "live by stealth"	Should
5. Technology Roadmap	• Support and provide technical leadership of projects and programmes to deliver the FSA's Technology roadmap • Work with other support partners to continually improve the technical infrastructure across all Service Groups • Work with FSA, and provide pro-active expertise, to identify opportunities for roadmap development and enhancement resulting from business change and industry innovations. • Enable the above by scheduling quarterly (as a minimum) Technology Review meetings with FSA	Must

Service Requirements

Description	Purpose	Priority
Service Availability	• Availability of services, and the support partner support *provision*, should be on a 24/7/365 basis, including core or 'working' hours 7:00am to 8:00pm Monday to Friday, and non-core 8:01pm to 6:59am Monday to Friday plus weekends and bank holidays	Must
Accessibility	• The support partner shall ensure that all services and documentation meet WCAG 2.1 AA accessibility standards for their area of responsibility	Must
User Access	• The support partner shall adhere to the FSA User Access policy. Role based user access must be supported and integration with Azure AD.	Must
GDPR	• The support partner must comply with their responsibilities under GDPR.	Must
Service Management	• The support partner shall work to the respective FSA processes for Acceptance into Service, Change management, Incident Management, Request Management, Knowledge Management, Problem Management, Service Asset and Configuration Management, and contribute as required for their areas of responsibility. • [FS430635_006 FSA Acceptance Into Service Procedure, • FS430635_007 FSA Change Management Procedure, • FS430635_008 FSA Incident Management Procedure, • FS430635_009 FSA Security Incident Procedure 2019, • FS430635_010 FSA Problem Management Process, • FS430635_011 FSA Knowledge Management Procedure,	Must

Description	Purpose	Priority
	• FS430635_012 FSA Service Asset & Configuration Management (SACM) Procedures, • FS430635_014 Service Capability High Level Principles, • FS430635_018 FSA Request Fulfilment,] • The support partner shall provide high- and low-level design documents for all services and solutions. These must be reviewed and updated on at least an annual basis and following the successful implementation of Changes, in line with the FSA knowledge management process • The support partner shall contribute to the review of services, evaluation, definition, execution and monitoring of CSI initiatives, ensuring these are appropriately recorded and reported against • ITIL principles must be followed • The support partner will work on the FSA ServiceNow instance with respect to all service management processes • The support partner shall participate in a monthly service review and shall report on their own performance, including but not limited to incident, request, change, problem management, Continual Service Improvements, Risk, Security, monitoring, SLA performance and any ongoing projects for their areas of responsibility • The support partner will work to Service Level Agreements as specified in the FSA Service Level Agreement document [FS430635_019 Service Level Agreements]	
Ways of working	• The support partner shall collaborate with the relevant FSA groups and other third-party support partners in line with the FSA collaboration charter, as well as participate in any testing and training as required	Must
Networking	• The Support partner will ensure that any FSA Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.	Must
Security	• The support partner shall ensure that all personnel are subject to the appropriate pre-employment checks and any additional vetting / national security vetting clearance as required. • The Supplier will follow FSA Access policies See attached [FS430635_013 FSA Supplier Access Policy August 2019 v1]	Must
Hosting and Location of FSA Data	• The Support partner shall ensure that they and none of their Sub-contractors Process FSA Data outside the EEA (including backups) without the prior written consent of the FSA.	Must

QUALIFICATION RESPONSES EVALUATION DETAILS (*)

Number of Responses	1
Number of Questions	24

Supplier	Methods Business & Digital Technology
Supplier Evaluation	Accepted
Acceptance or Rejection Notes	

Section Name	1.1 Essential requirements for this service

Note	Note Details
1.1.1 Qualification responses	If you answer No to any of the below Service qualification questions please do not respond to this Invitation to Tender.
Response	

Question	Description
1.1.2 Capability	Please confirm that you have the capability to design, build and operate a multi-cloud estate.
Response	
Yes	

Question	Description
1.1.3 Fully Managed service	Please confirm that you can provide a full managed service, including all aspects of services, databases management (including SQL), data storage and infrastructure.
Response	
Yes	

Question	Description
1.1.4 Azure Experience	Please confirm that you can demonstrate experience of managing a Microsoft Azure tenancy.
Response	
Yes	

Question	Description
1.1.5 Multi-Supplier working	Please confirm that you have experience working in a multi-Supplier model. For example, dependant on other suppliers while those Suppliers also have dependencies on you as a Support Partner.
Response	

Yes

Question	Description
1.1.6 Accessibility	Please confirm that you shall ensure that all services and documentation meet WCAG 2.1 AA accessibility standards for their area of responsibility.

Response
Yes

Question	Description
1.1.7 Service availability	Please confirm that availability of services will be on a 24 hours a day, 7 days a week, 365 days a year basis, except where specified with FSA agreement.
Response	
Yes	

Question	Description
1.1.8 Working hours	Please confirm that you will provide a 24/7/365 service, including core or 'working' hours 7:00am to 8:00pm Monday to Friday , and non-core 8:01pm to 6: 59am Monday to Friday plus weekends and bank holidays
Response	
Yes	

Question	Description
1.1.9 ITSM Toolset (ServiceNow)	Please confirm you will work within the FSA ServiceNow instance with respect to all service management processes.
Response	
Yes	

Section Name	1.2 Security Requirements

Note	Note Details
1.2.1 Security Qualification responses	If you answer No to any of the below Security Qualification questions please do not respond to this Invitation to Tender.
Response	

Question	Description
1.2.2 Personnel Security	All Supplier Personnel will be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.3 Identity, Authentication and Access Control	Please confirm that you will provide an access control regime that ensures all users and administrators of the Supplier System/Service are uniquely identified and authenticated when accessing or administering the Services.
Response	

Yes

Question	Description
1.2.4 Identity, Authentication and Access Control	Please confirm that you will apply the 'principle of least privilege' when setting access to the Supplier System/Service so that access is set for only parts of the Supplier System/service they require.
Response	
Yes	

Question	Description
1.2.5 Event Logs and Protective Monitoring	Please confirm that you shall collect audit records which relate to security events that would support the analysis of potential and actual compromises.
Response	
Yes	

Question	Description
1.2.6 Hosting and Location of FSA Data	The Supplier shall ensure that they and none of their Sub-contractors Process FSA Data outside the EEA (including back ups) without the prior written consent of the FSA. Please confirm that you agree to this.
Response	
Yes	

Question	Description
1.2.7 Secure Architecture	Please confirm you will ensure services are designed in accordance with the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;
Response	
Yes	

Question	Description
1.2.8 Secure Architecture	Please confirm you will ensure services are designed in accordance with the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main
Response	
Yes	

Question	Description
1.2.9 Secure Architecture	Please confirm will ensure services are designed in accordance with the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
Response	
Yes	

Question	Description
1.2.10 Protection for Digital Services	Please confirm you will ensure externally facing services have DDoS protection
Response	

Yes

Question	Description
1.2.11 Protection for Digital Services	Please confirm you will ensure externally facing services have a Web Access Firewall
Response	
Yes	

Question	Description
1.2.12 Principles of Security	The Supplier shall be responsible for the confidentiality, integrity and availability of FSA data whilst it is under the control of the Supplier and consequentially the security of the system/service. Please confirm you accept this.
Response	
Yes	

Question	Description
1.2.13 Certification	Please confirm you have Cyber Essentials PLUS
Response	
Yes	

Question	Description
1.2.14 Assurance	Please confirm you will create an information Security Management Document Set to document how they will comply with the specific FSA security requirements to be approved by the Head of Security at the FSA
Response	
Yes	

Question	Description
1.2.15 Incident and Breach Management - reporting	If the Supplier becomes aware of a Breach of Security covering FSA data (including a Personal data breach) the Supplier will inform the FSA at the earliest opportunity. Please confirm you accept this.
Response	
Yes	

Crown Commercial

Operational ITT Response

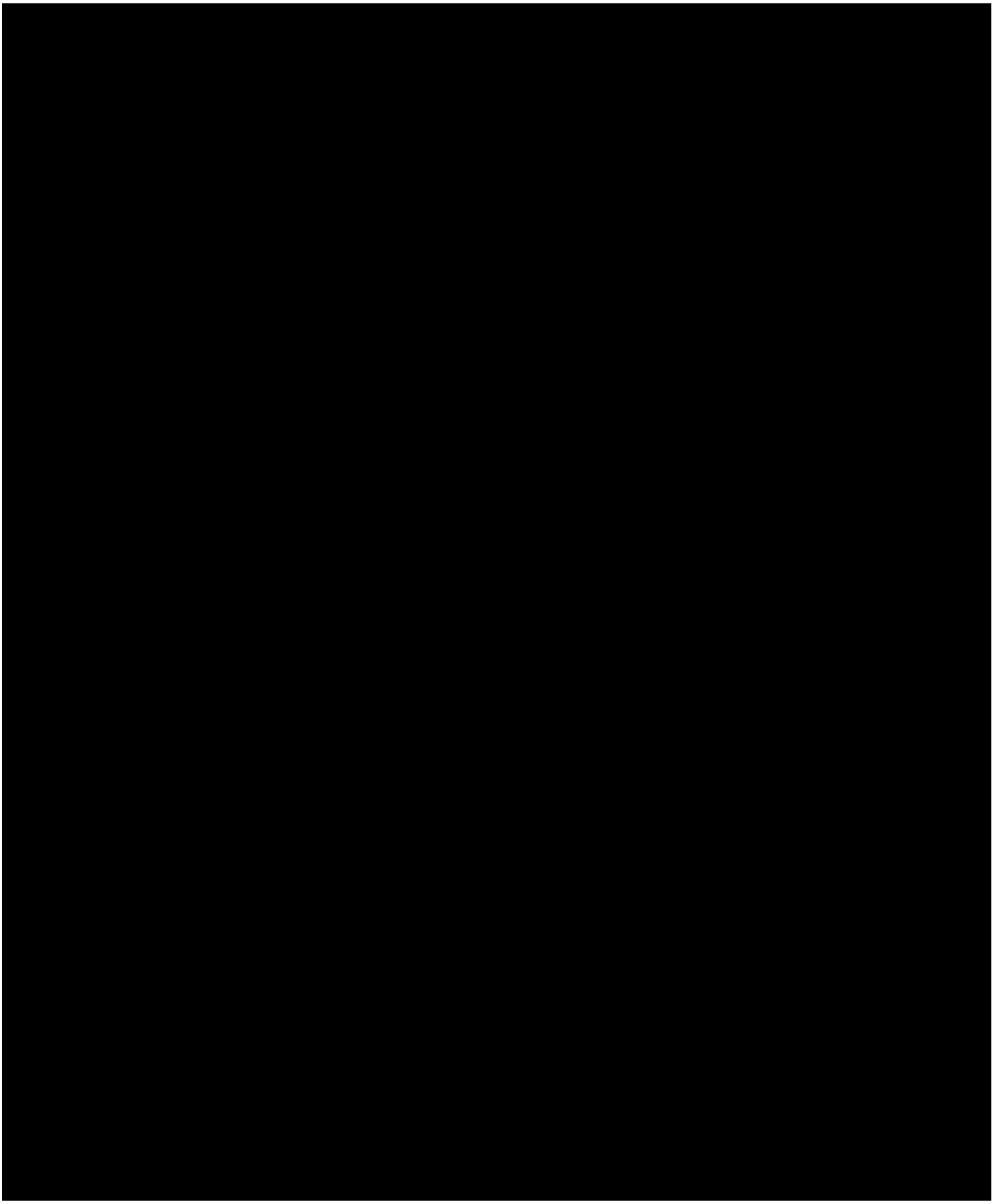
[redacted]

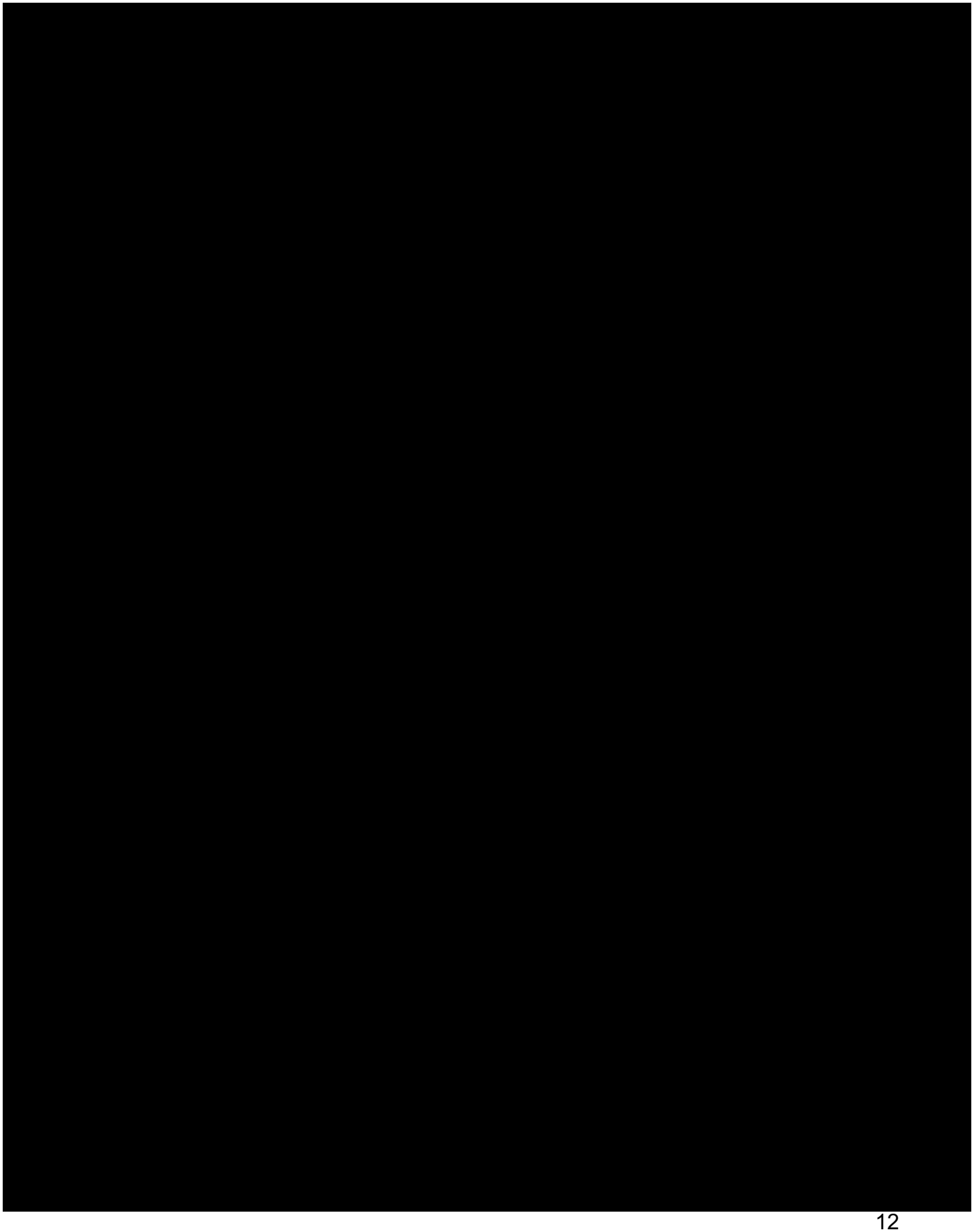
Crown
Commercial

[redacted]

Crown
Commercial

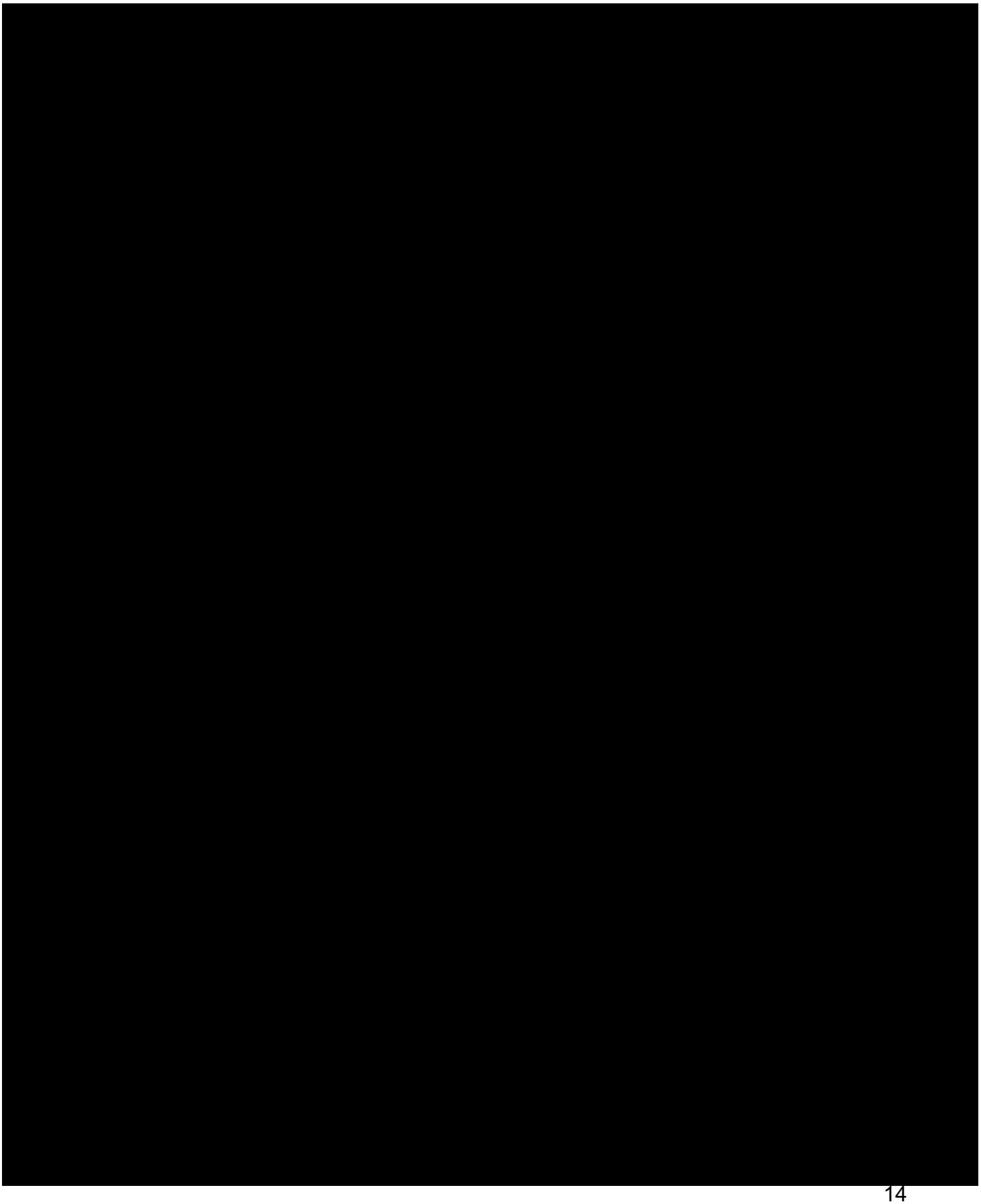
[redacted]





Crown
Commercial

[redacted]

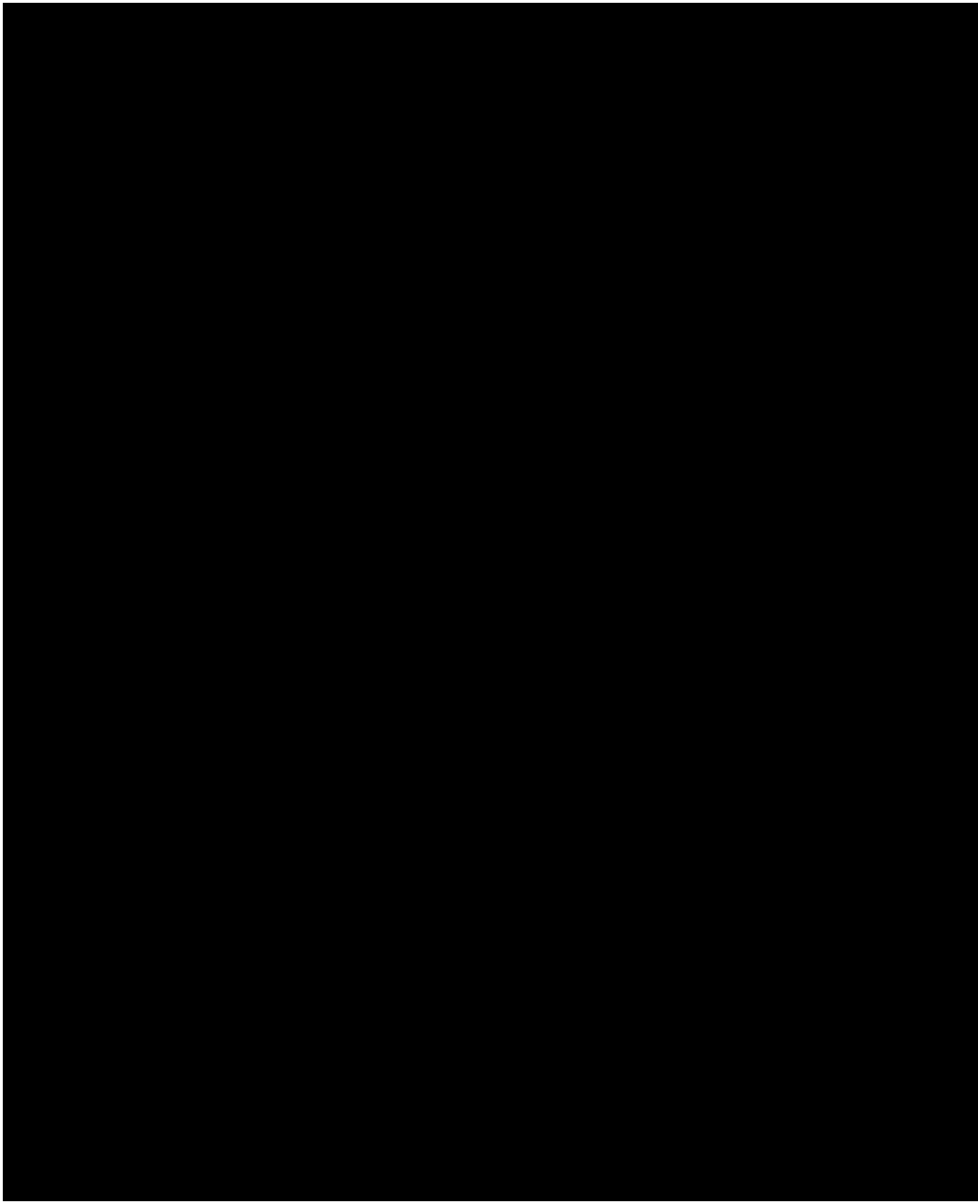


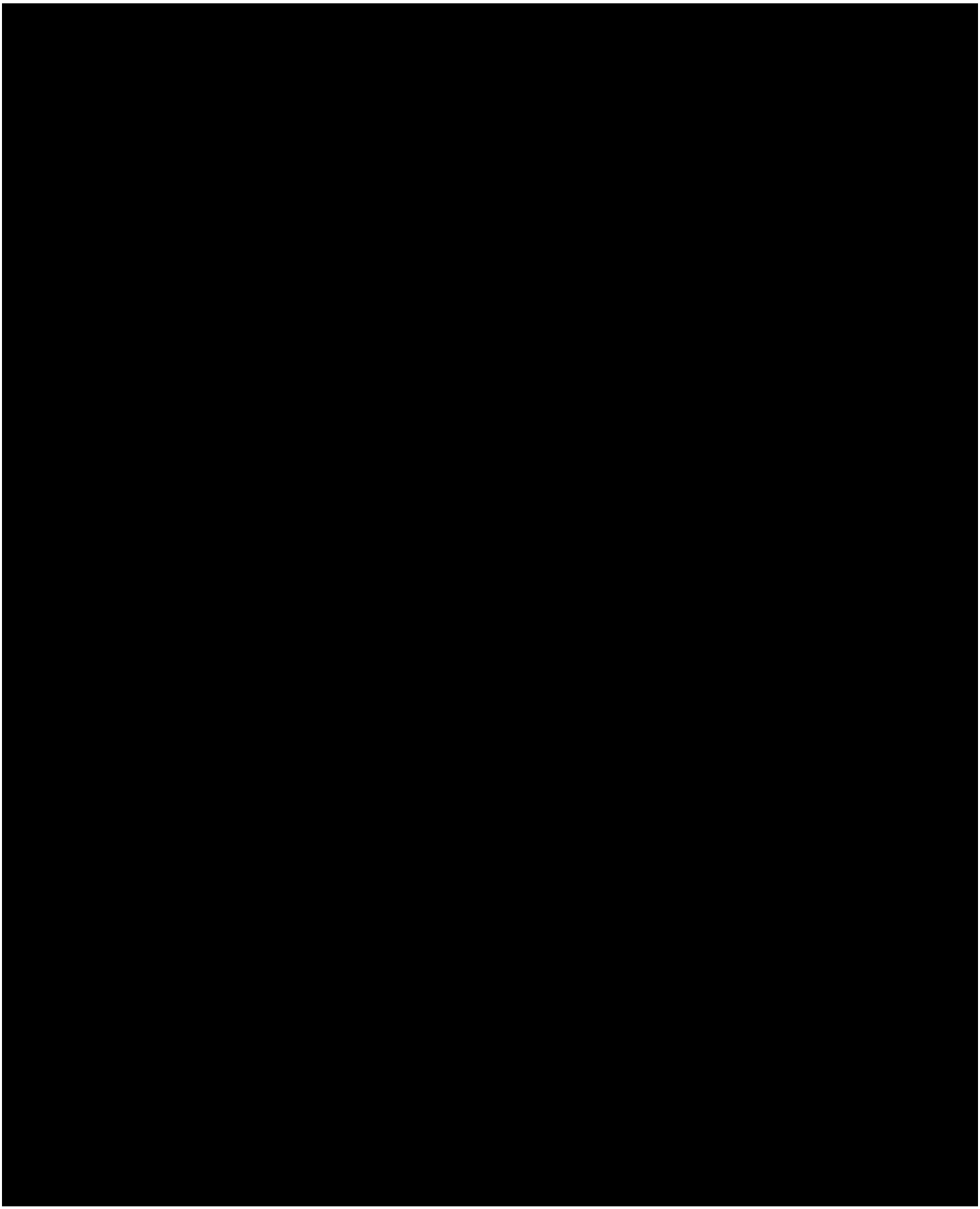
Crown
Commercial

[redacted]

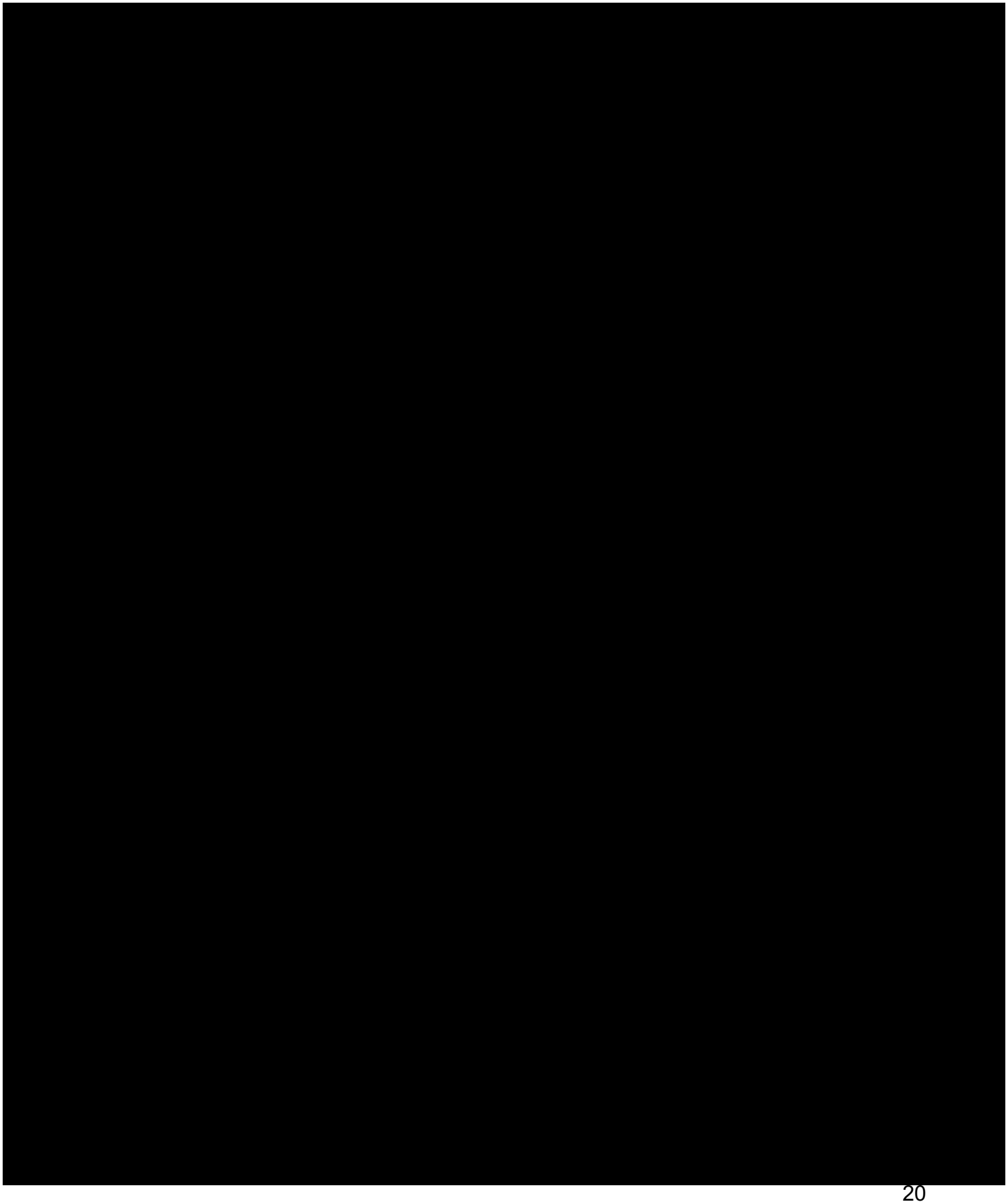
Crown
Commercial

[redacted]



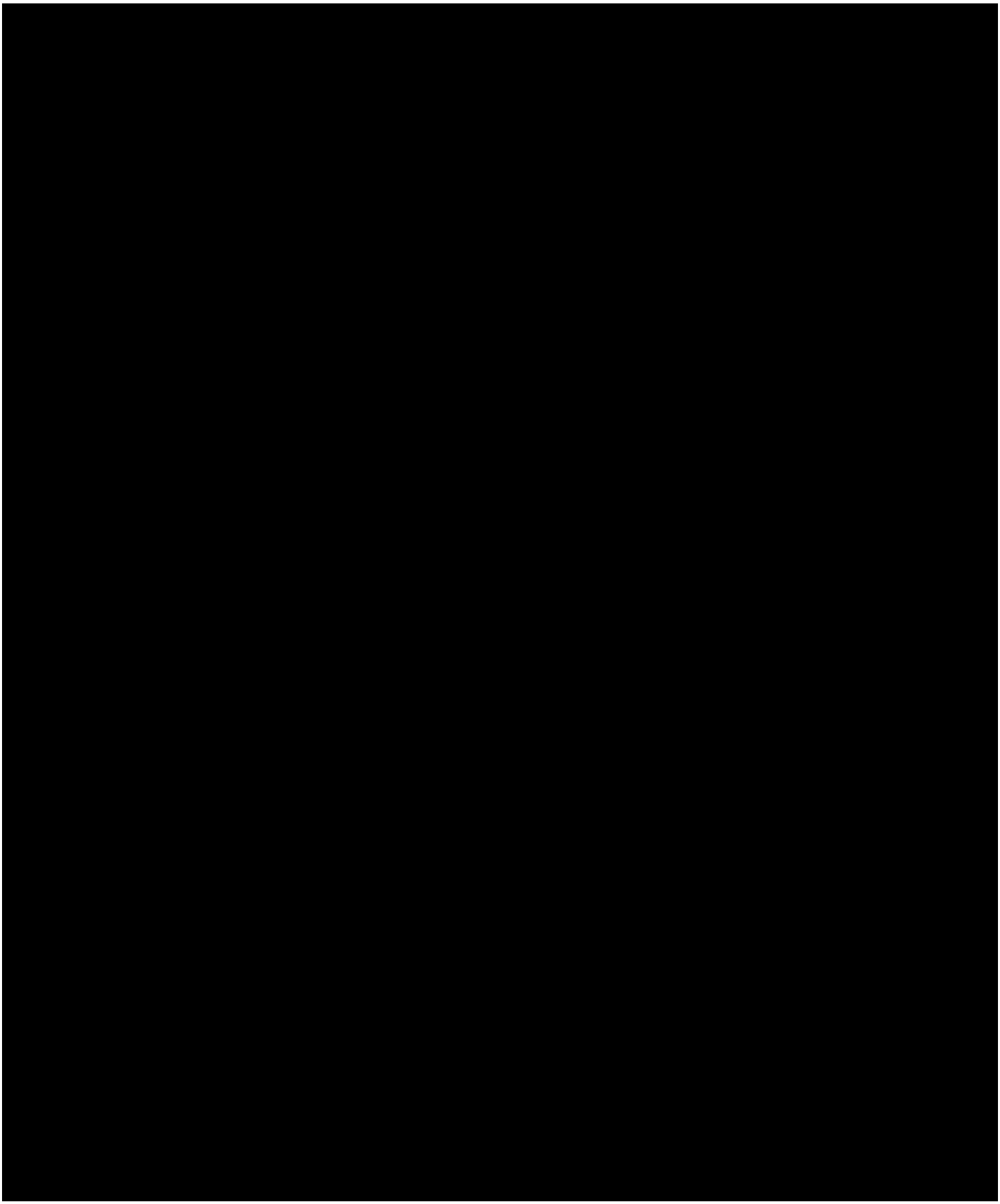


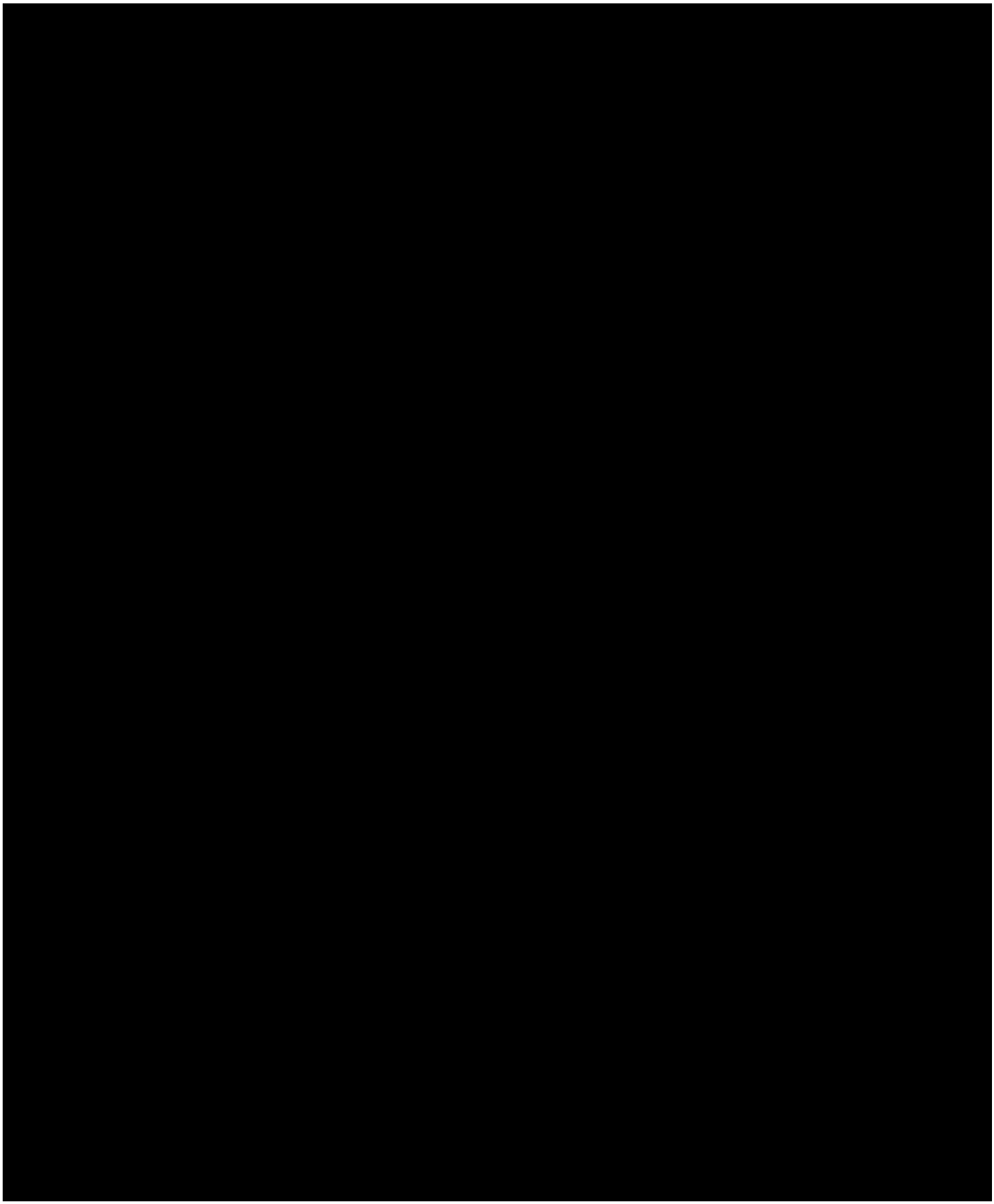
[redacted]

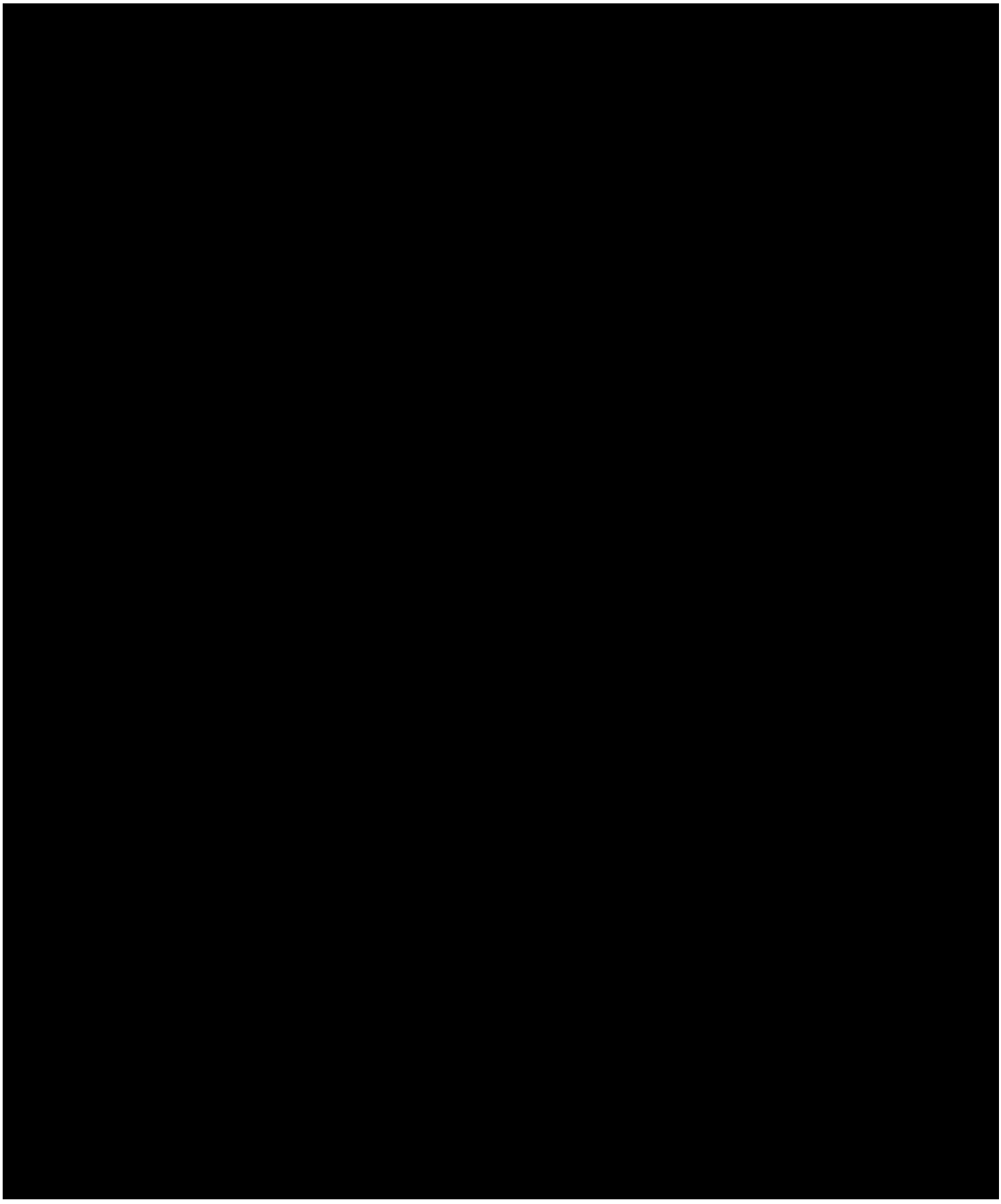


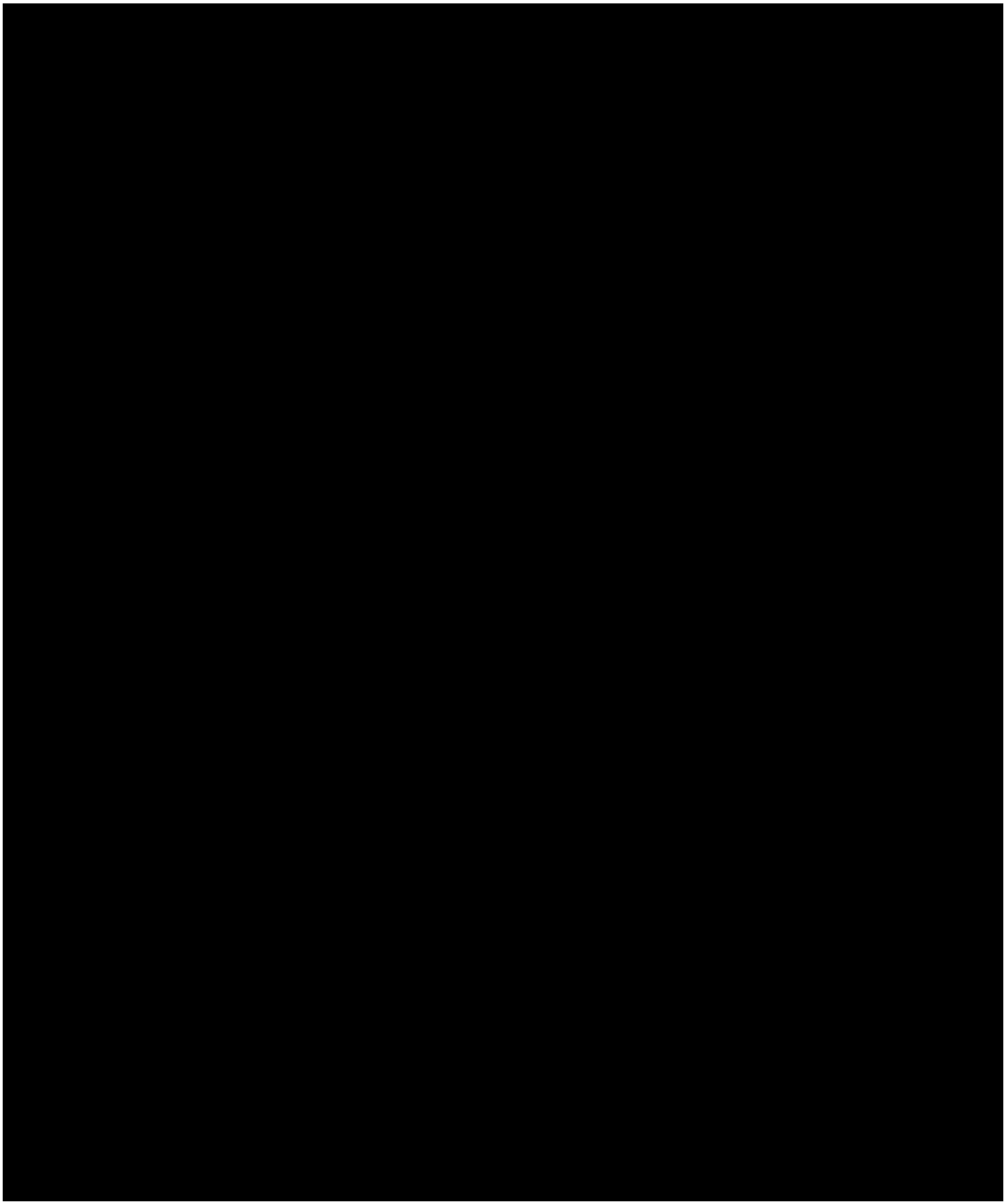
Crown
Commercial

[redacted]



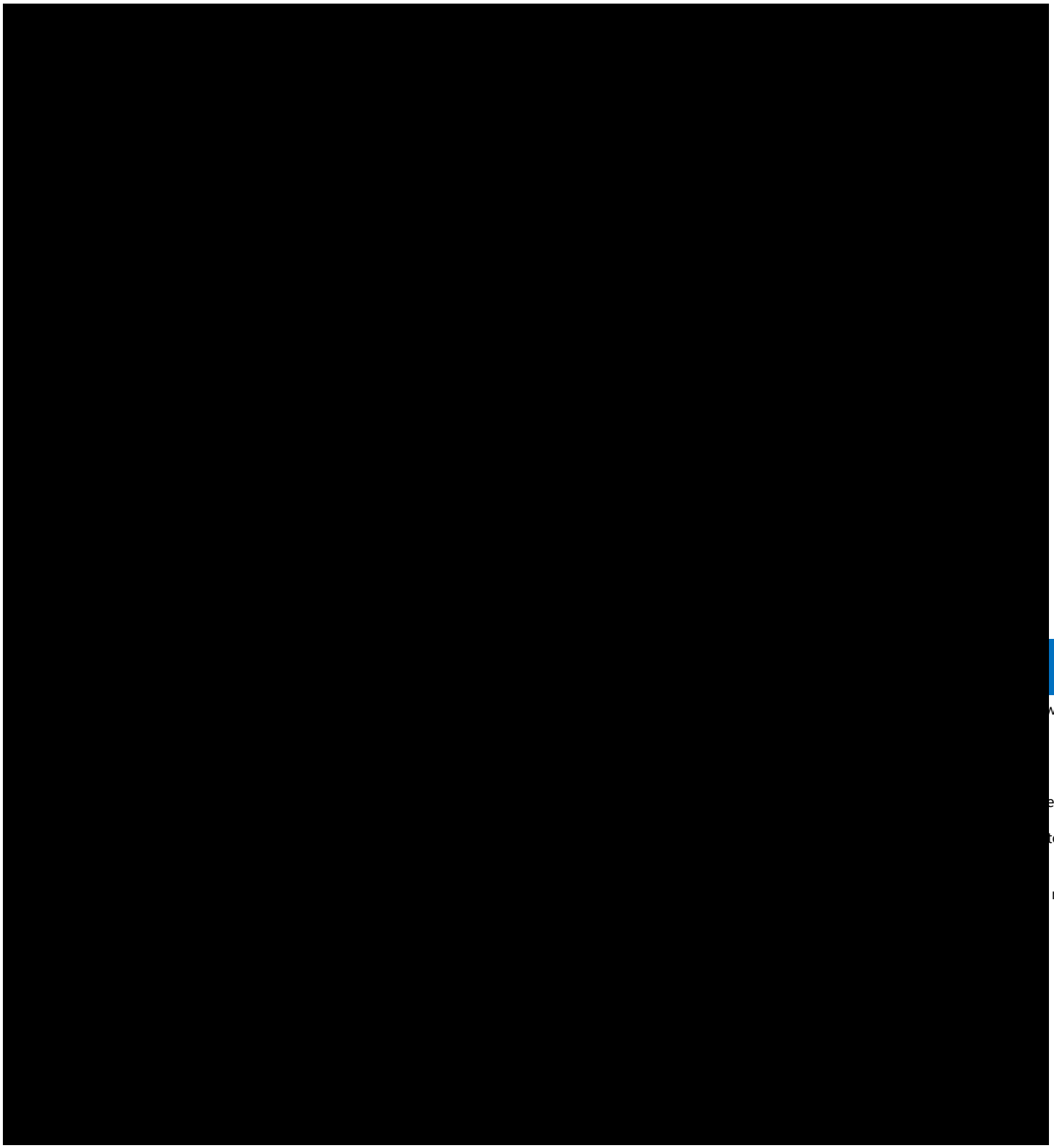




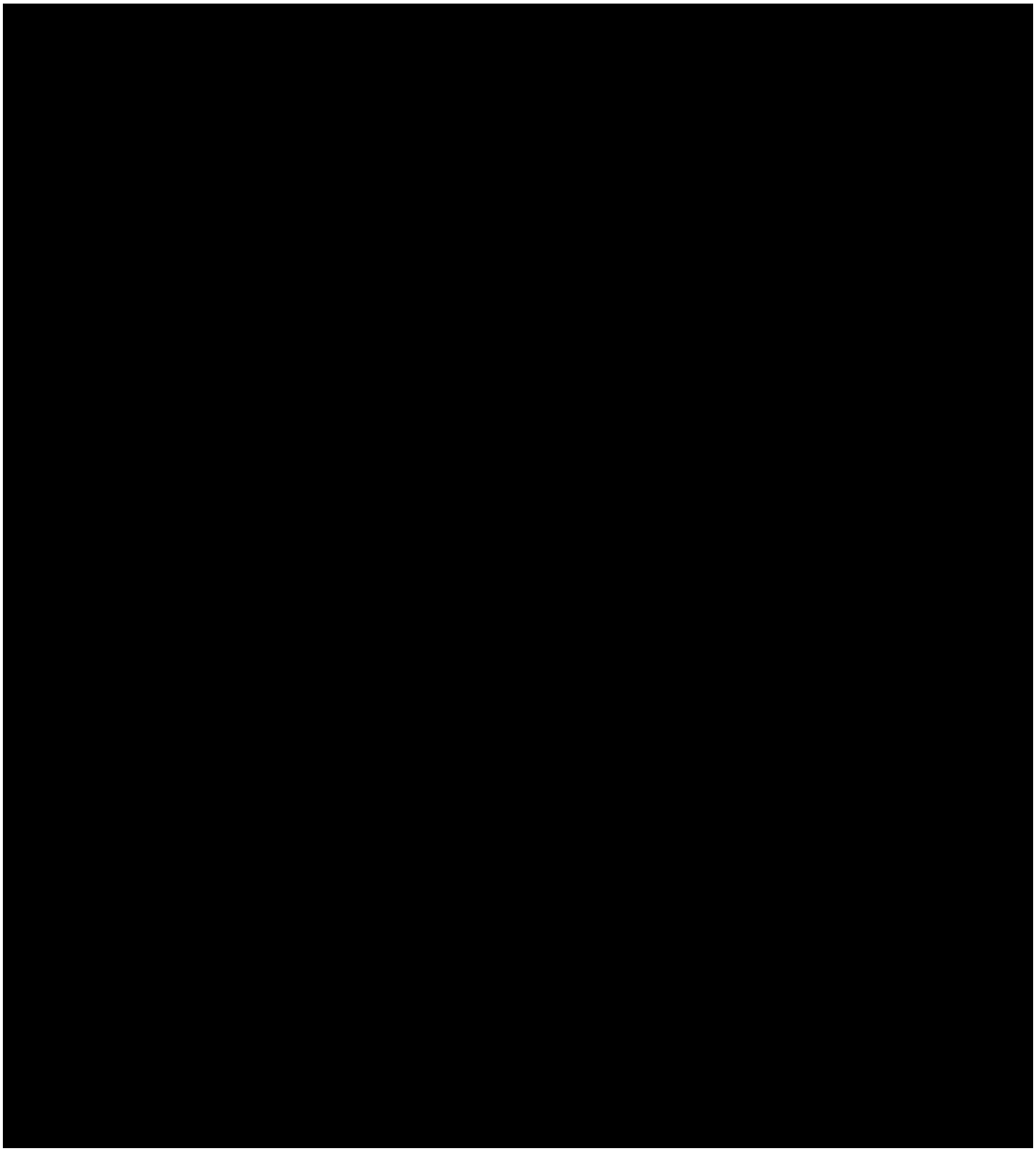


[redacted]

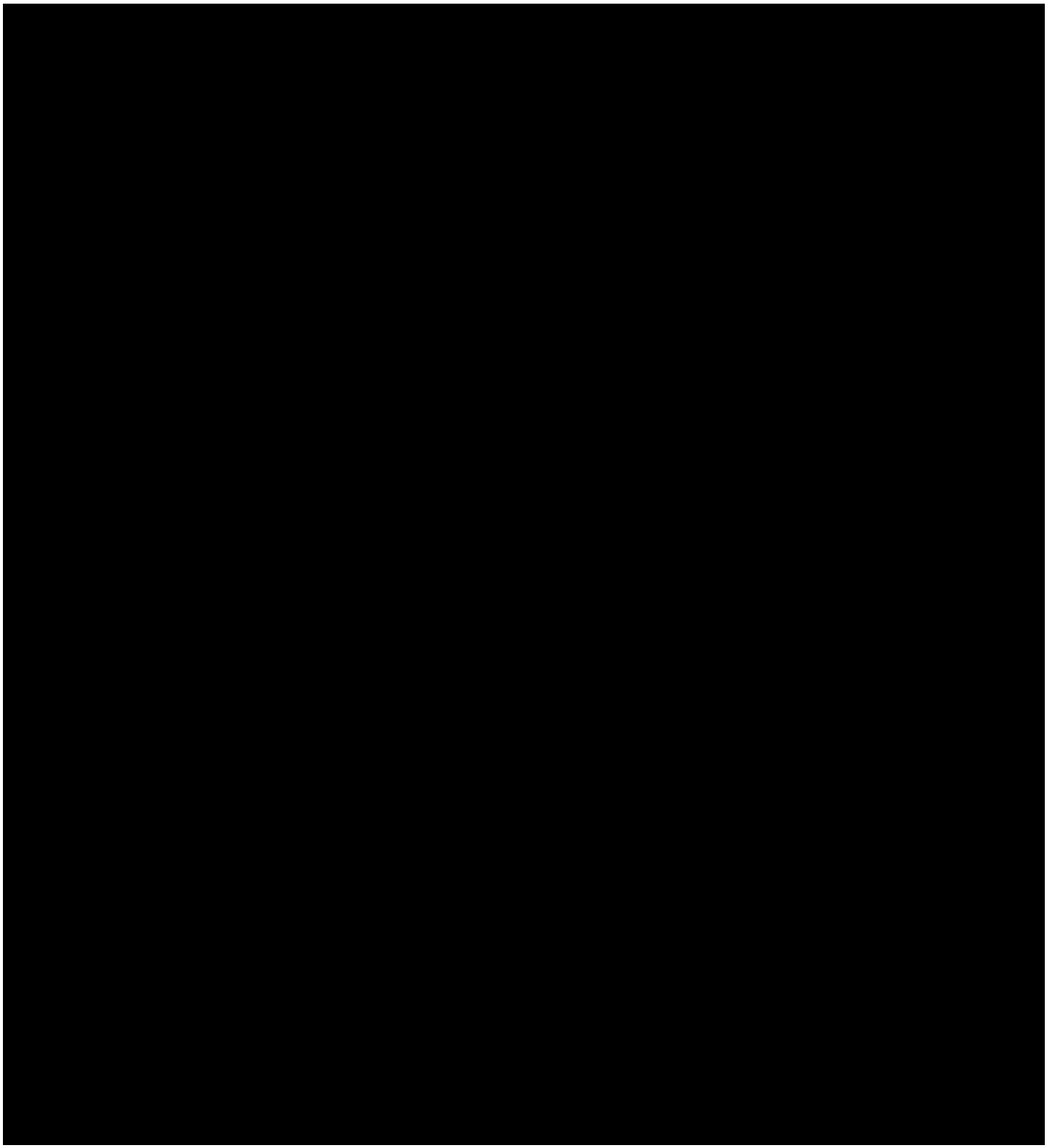
Crown Commercial

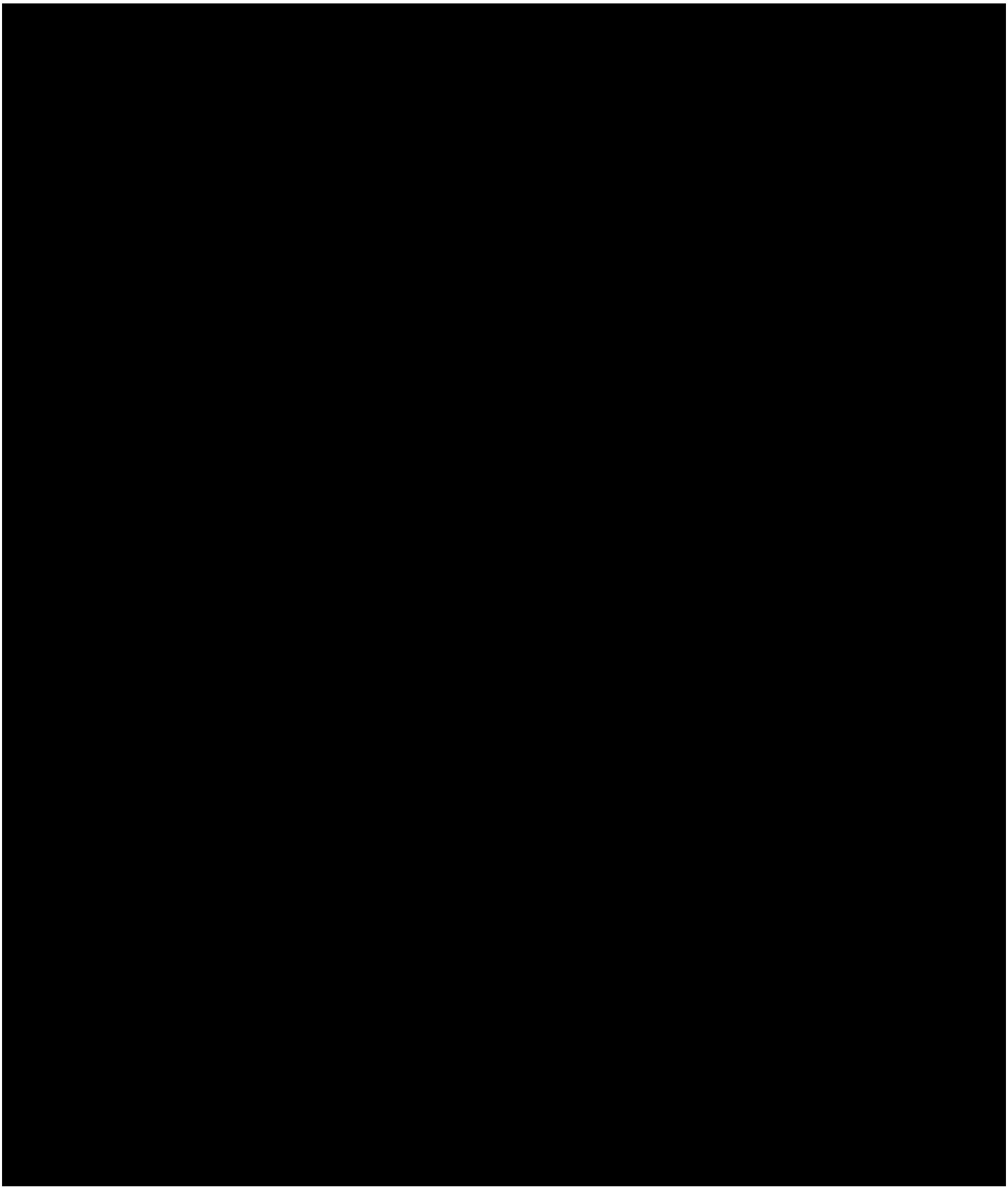


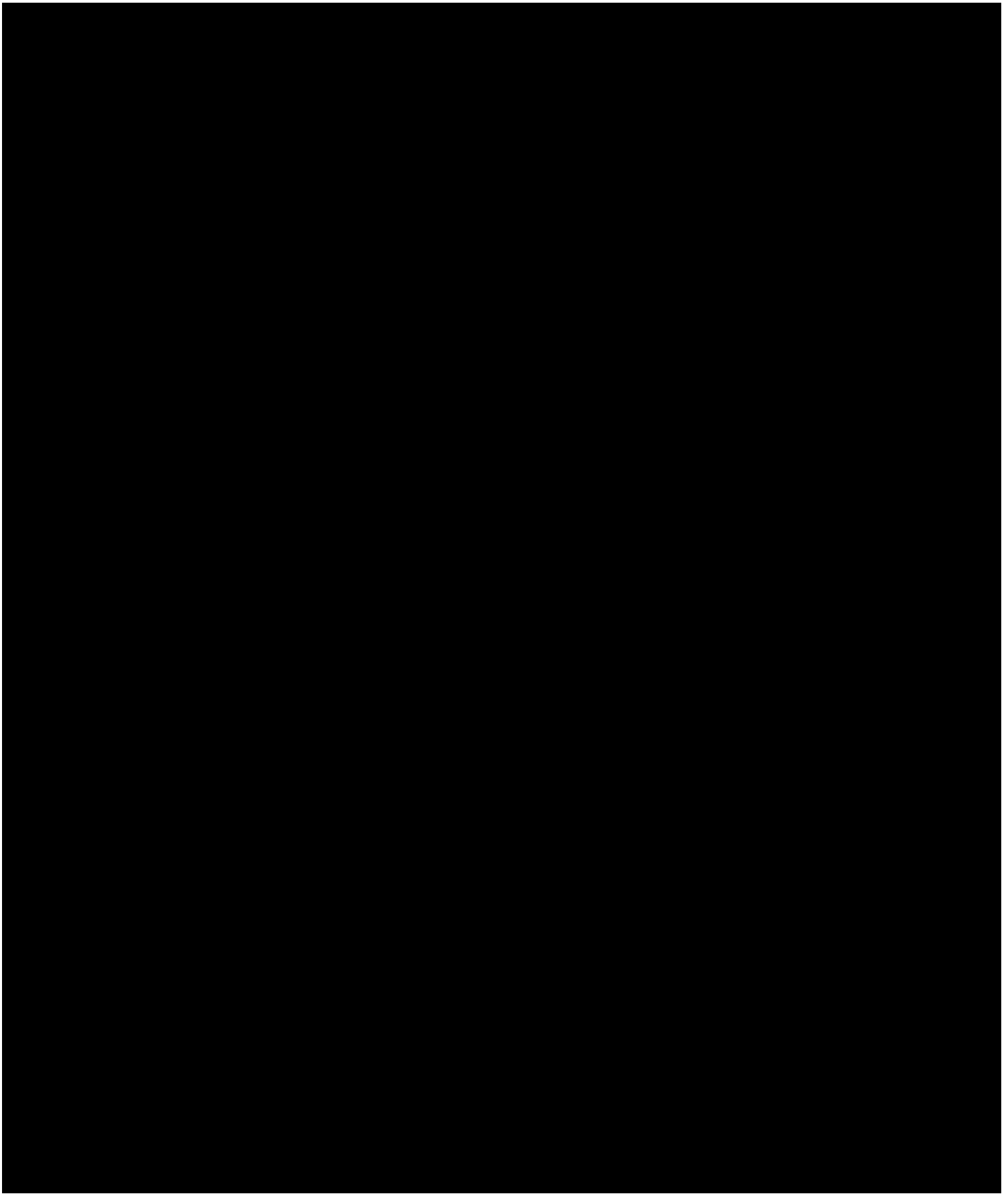
Crown Commercial



Crown Commercial



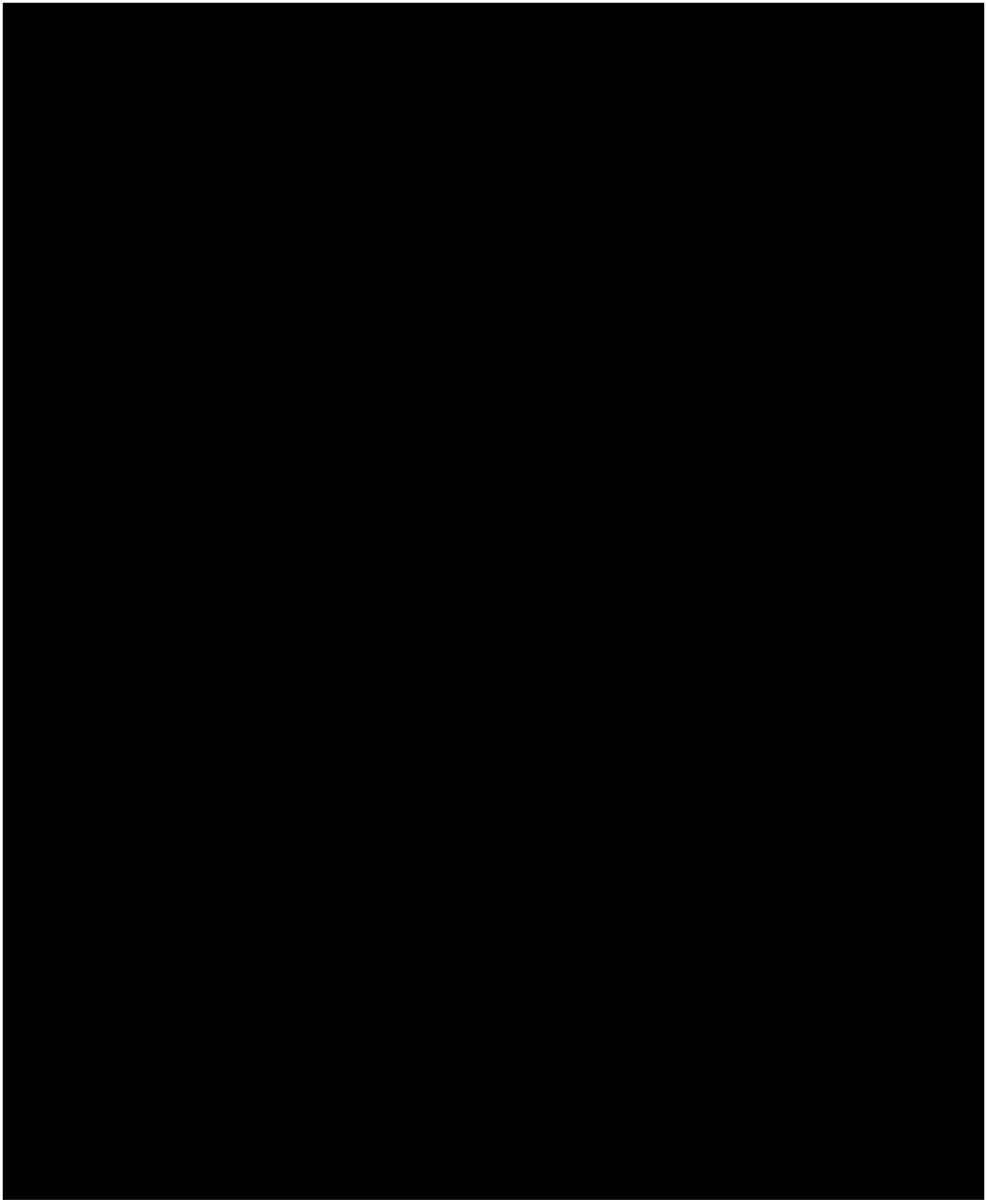




Crown
Commercial

[redacted]

Crown Commercial



Crown
Commercial

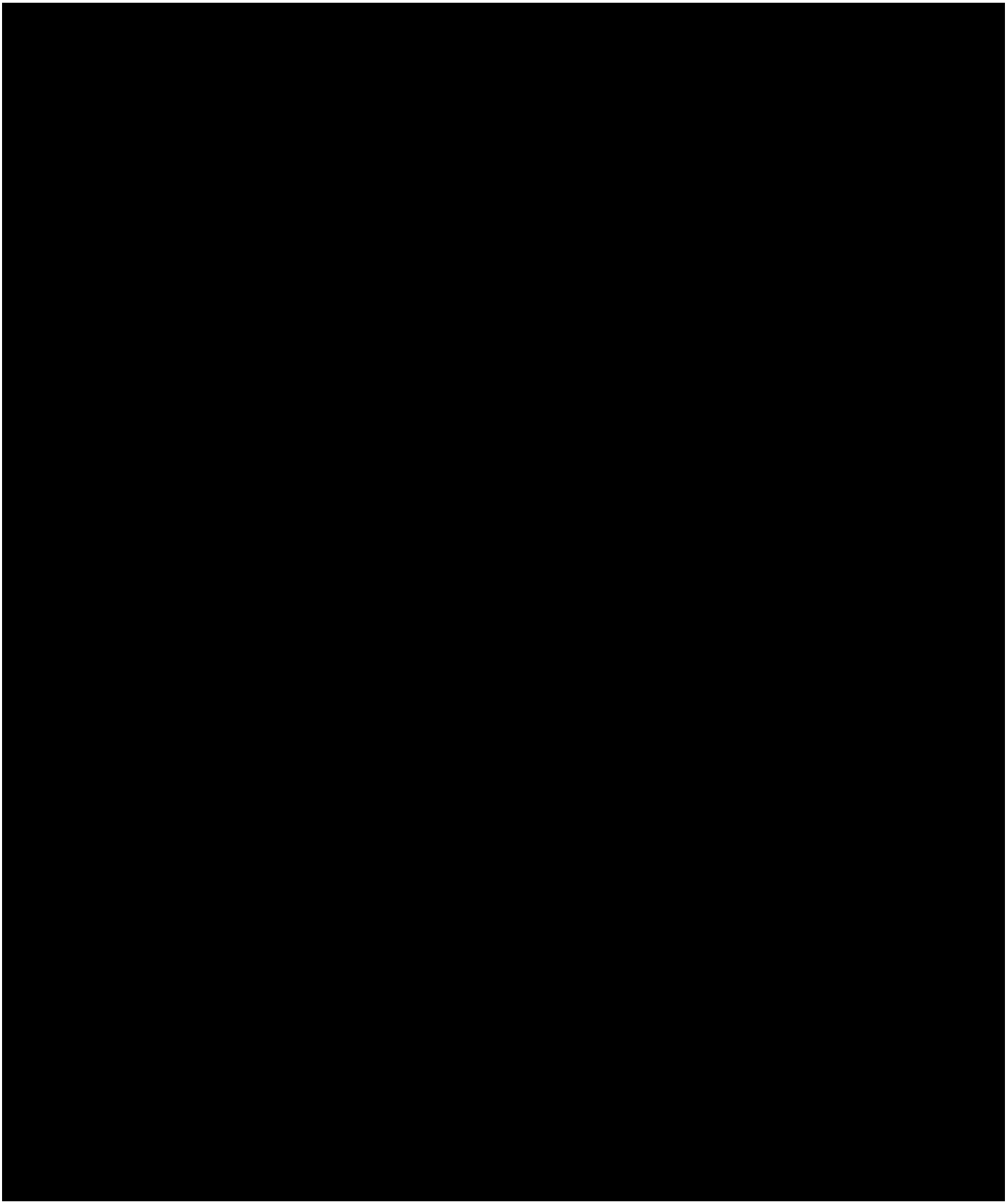
[redacted]

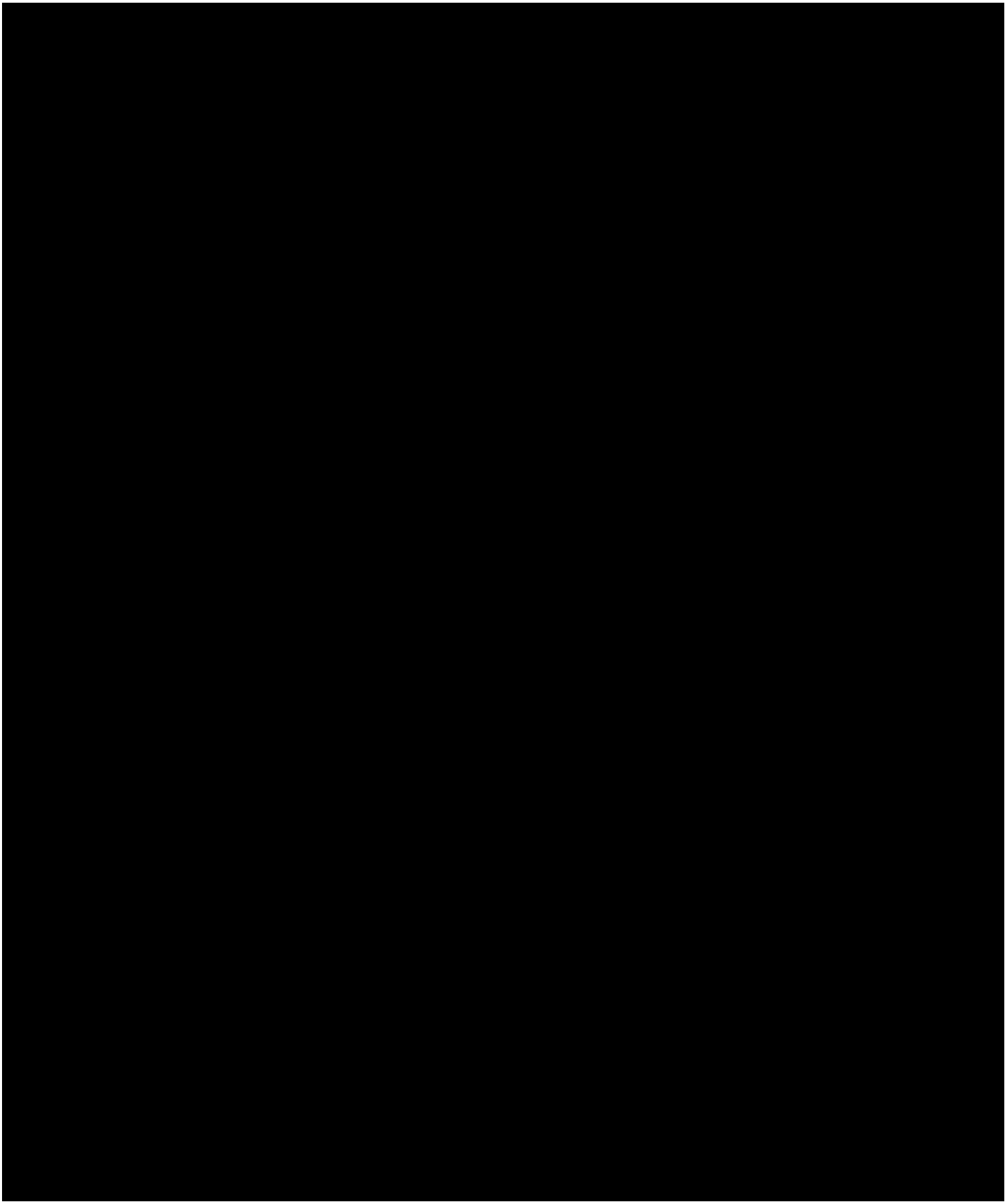
Crown
Commercial

[redacted]

Crown
Commercial

[redacted]



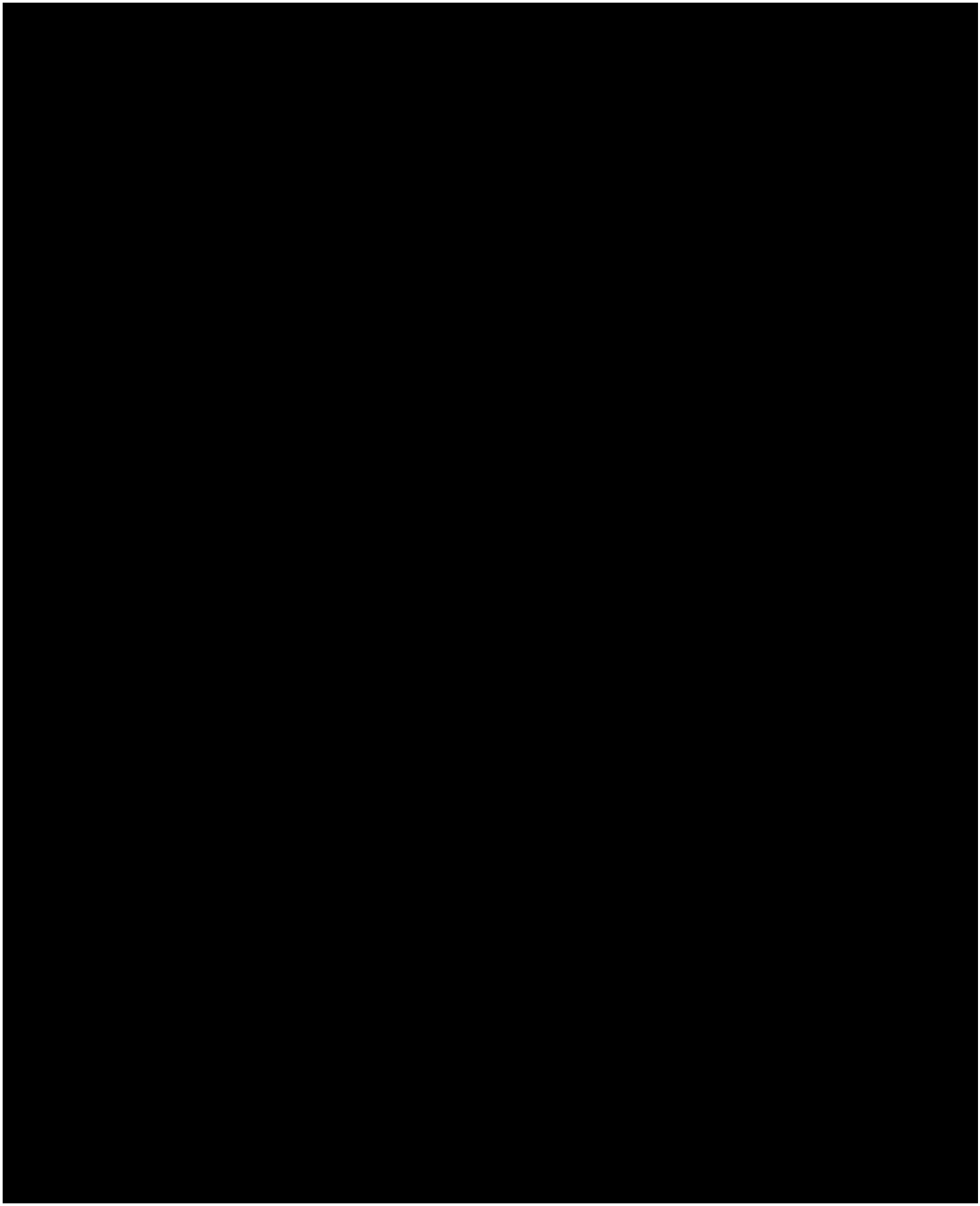


Crown
Commercial

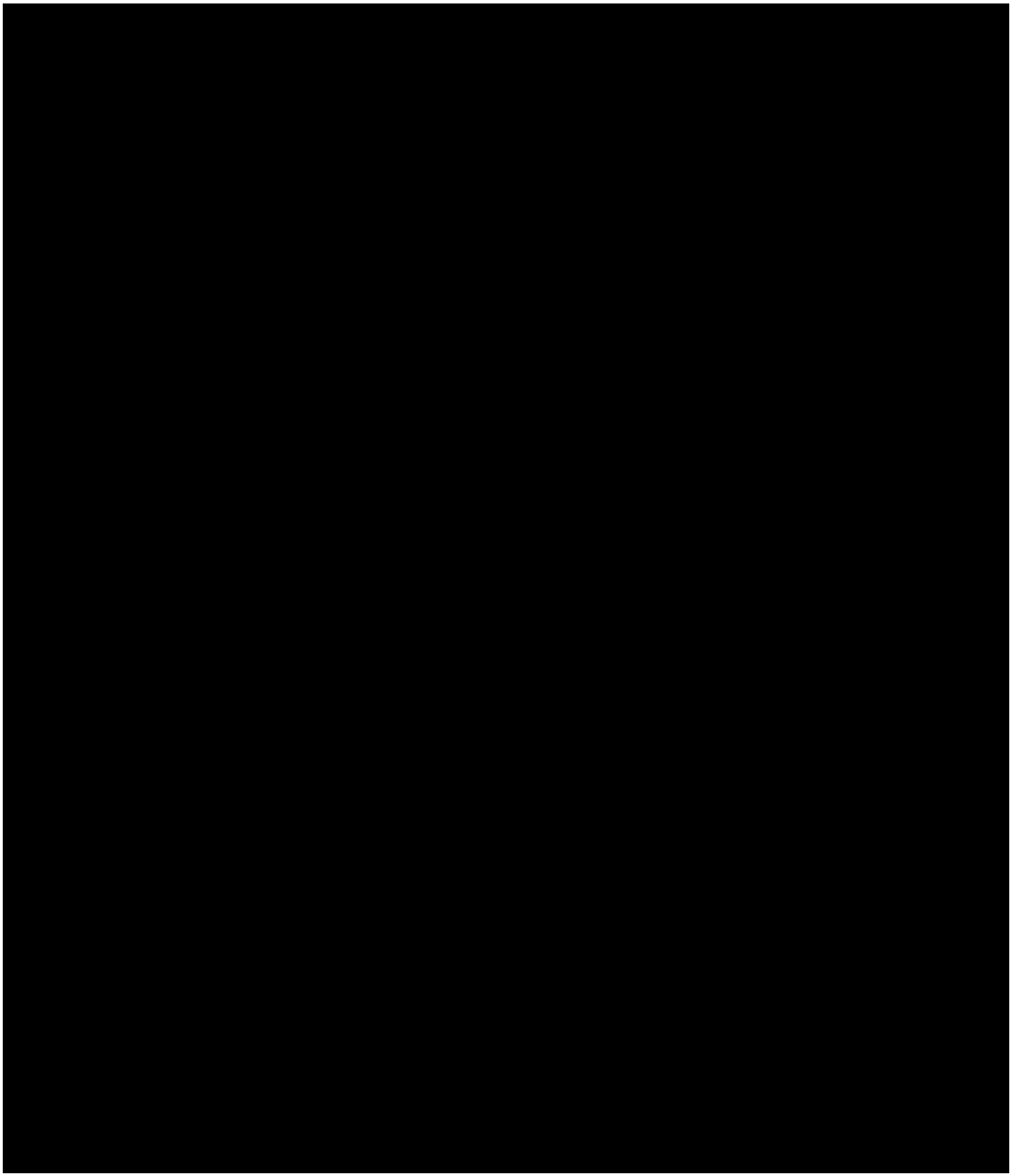
[redacted]

Crown
Commercial

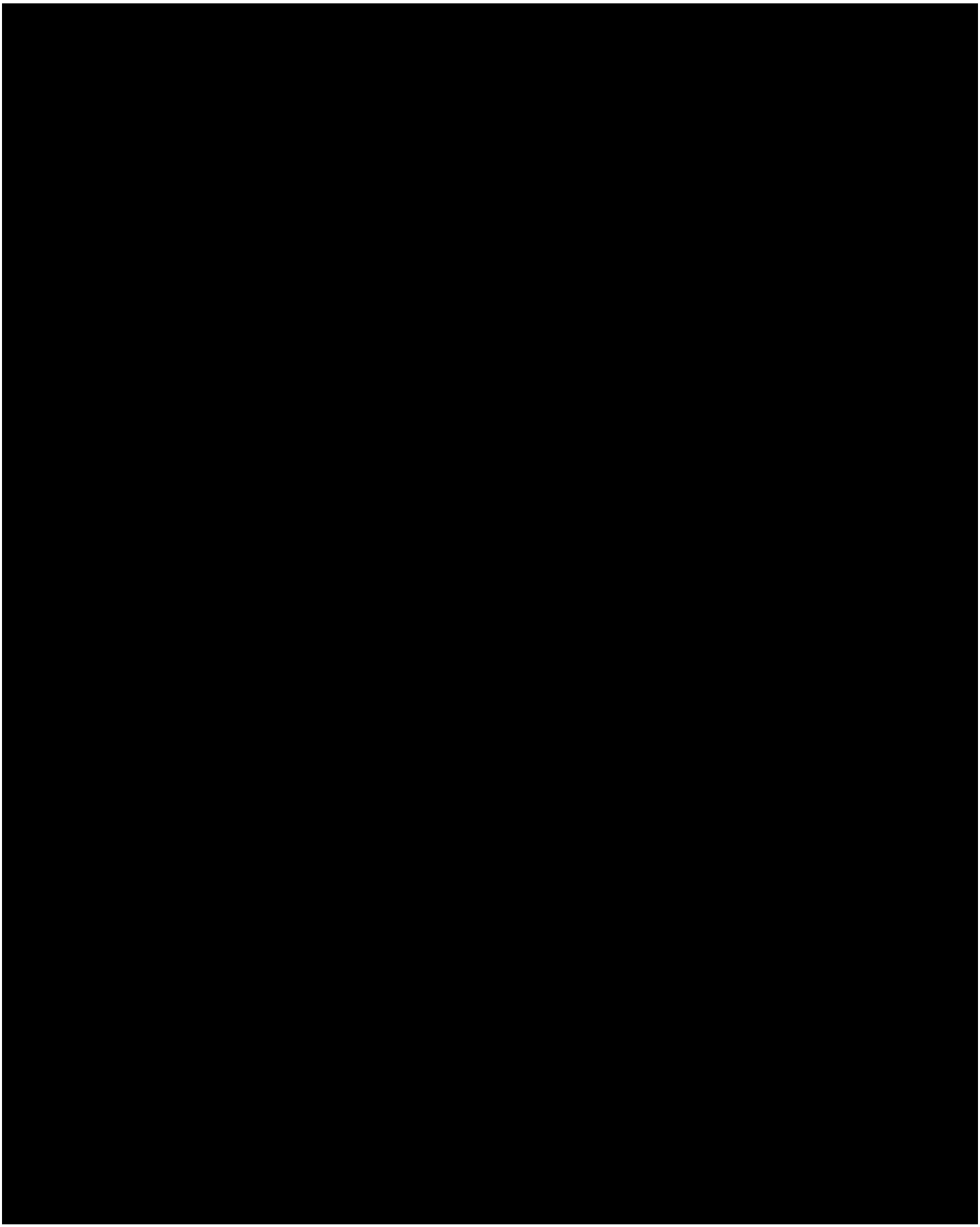
[redacted]

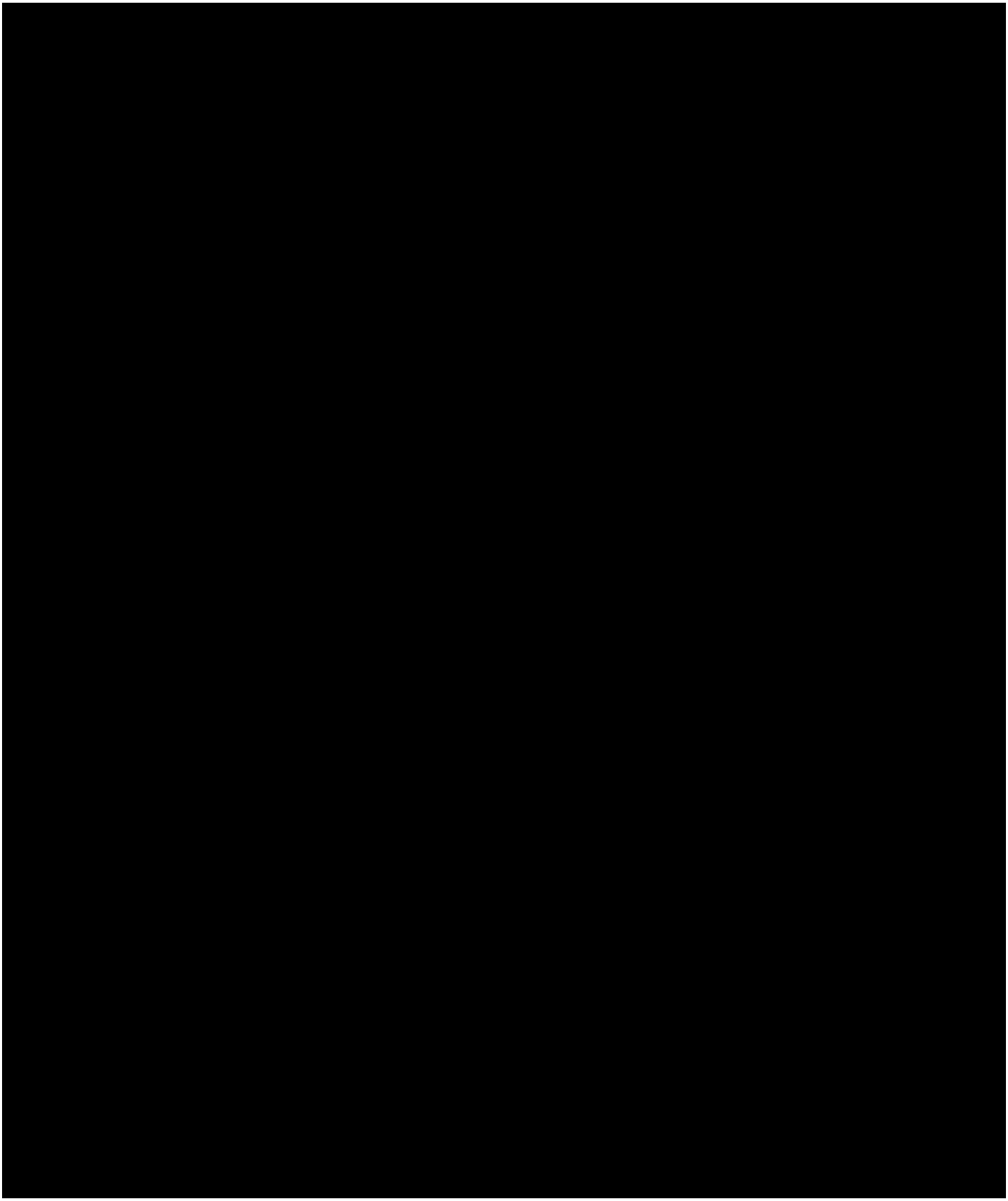


Crown Commercial



Crown
Commercial



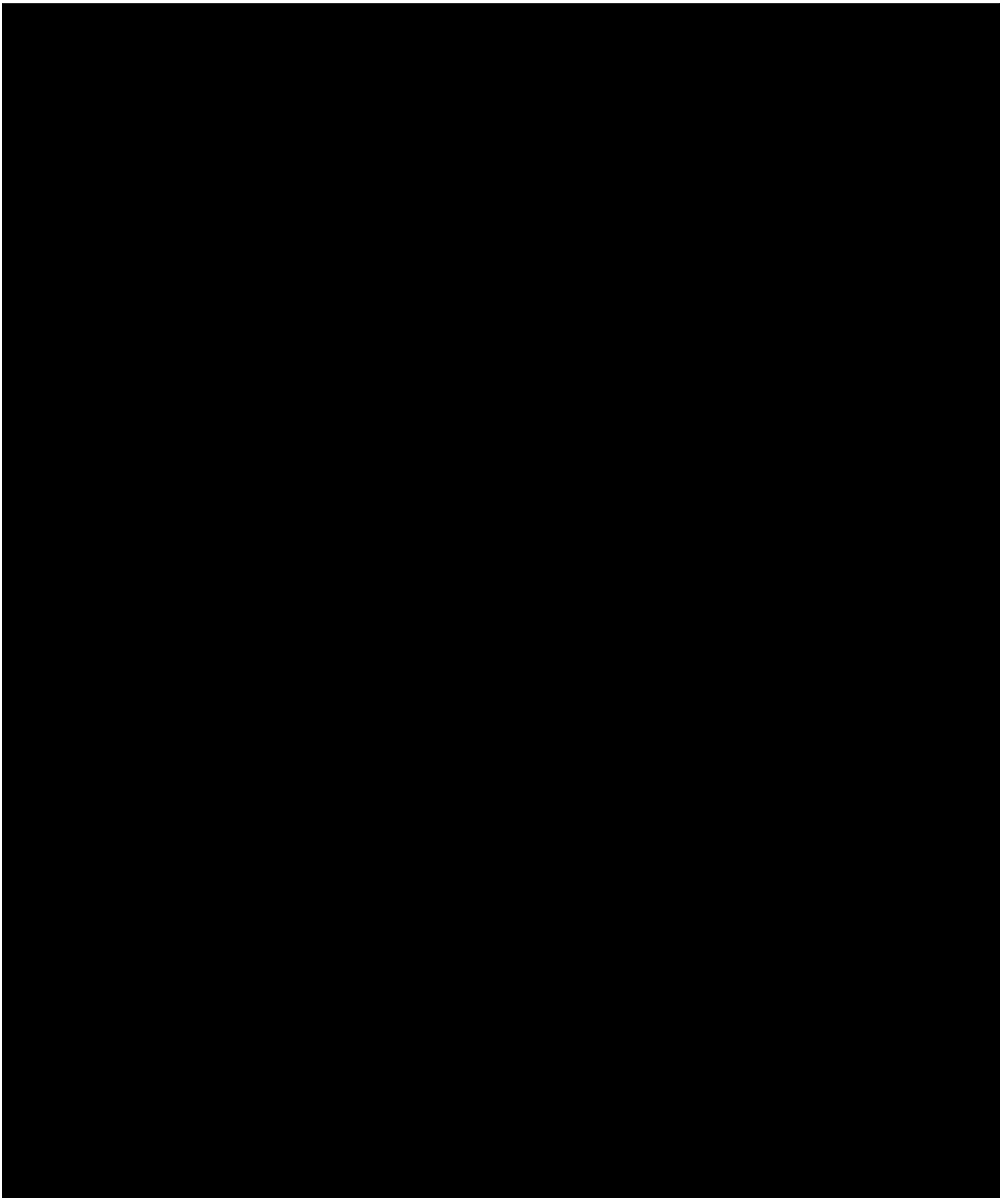


Crown
Commercial

[redacted]

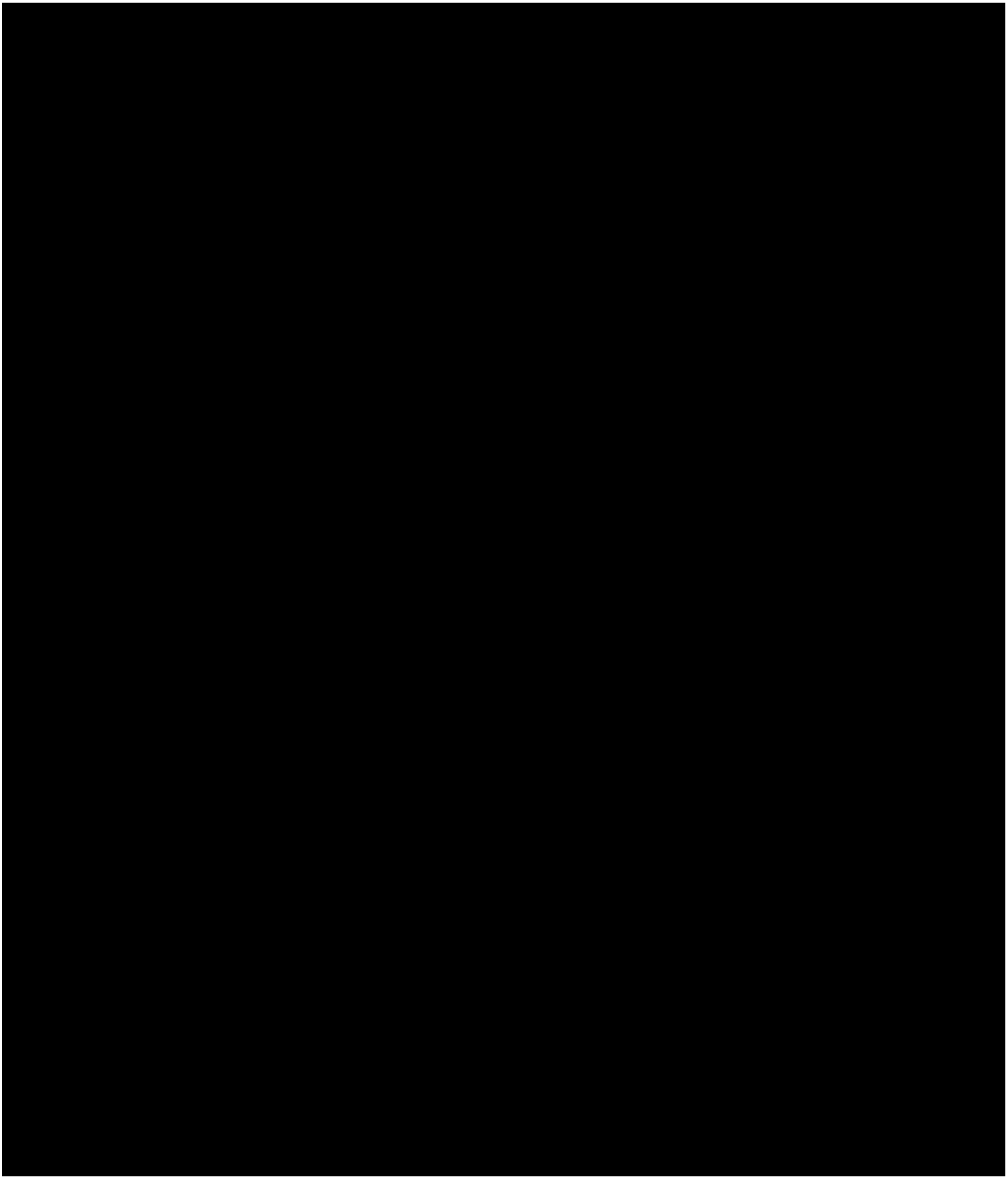
Crown
Commercial

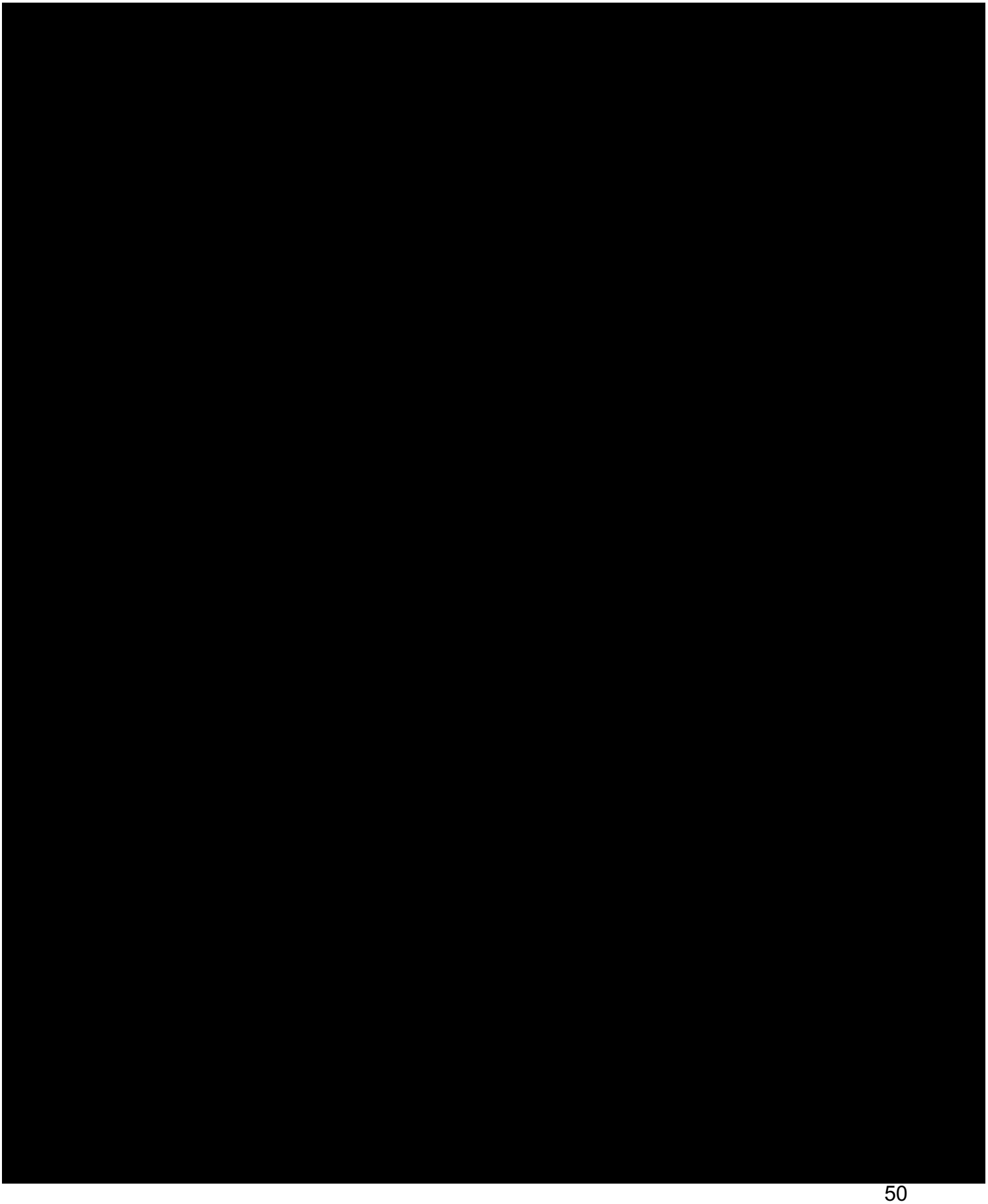
[redacted]



Crown
Commercial

[redacted]





Crown
Commercial

[redacted]

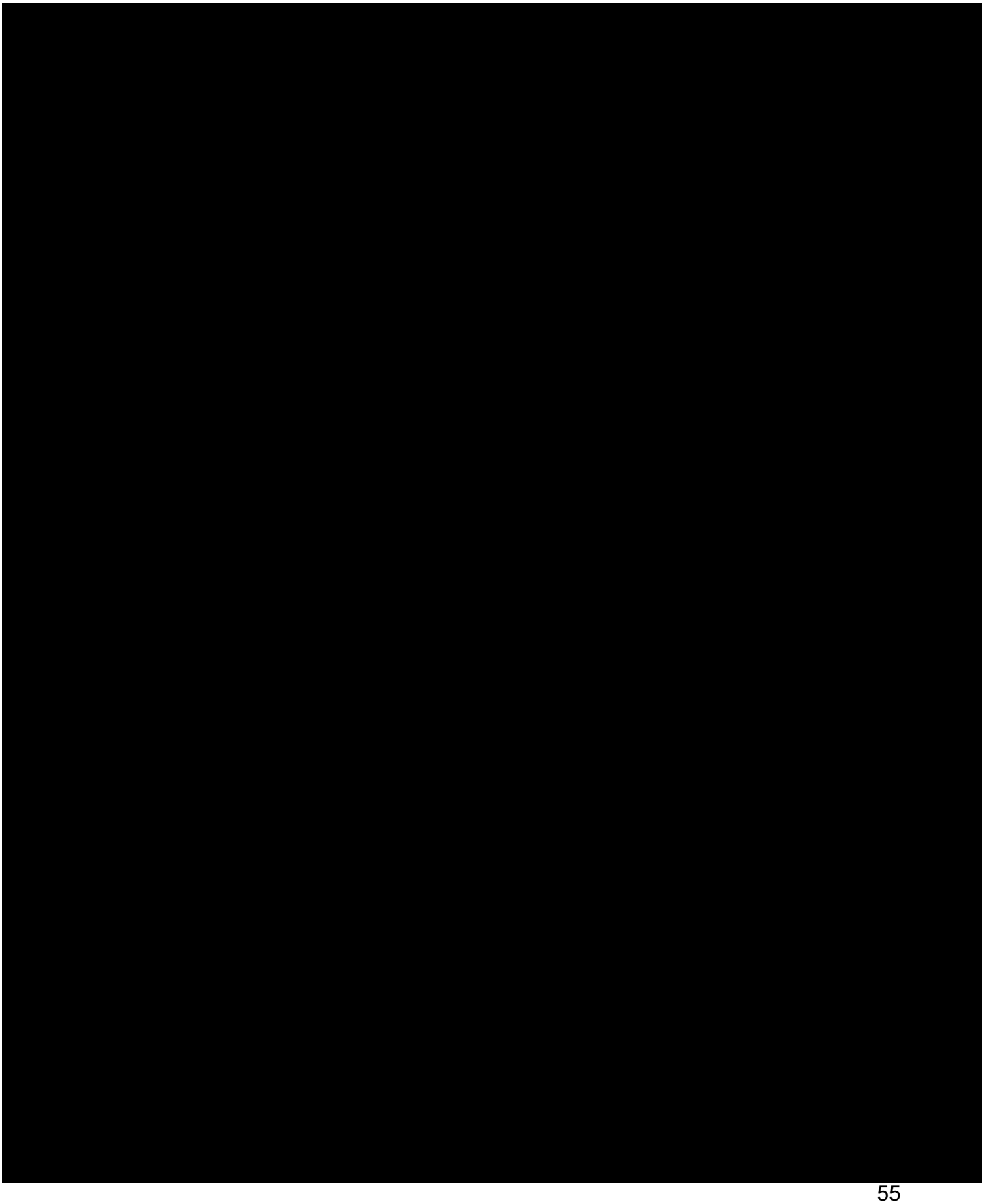
Crown
Commercial

[redacted]

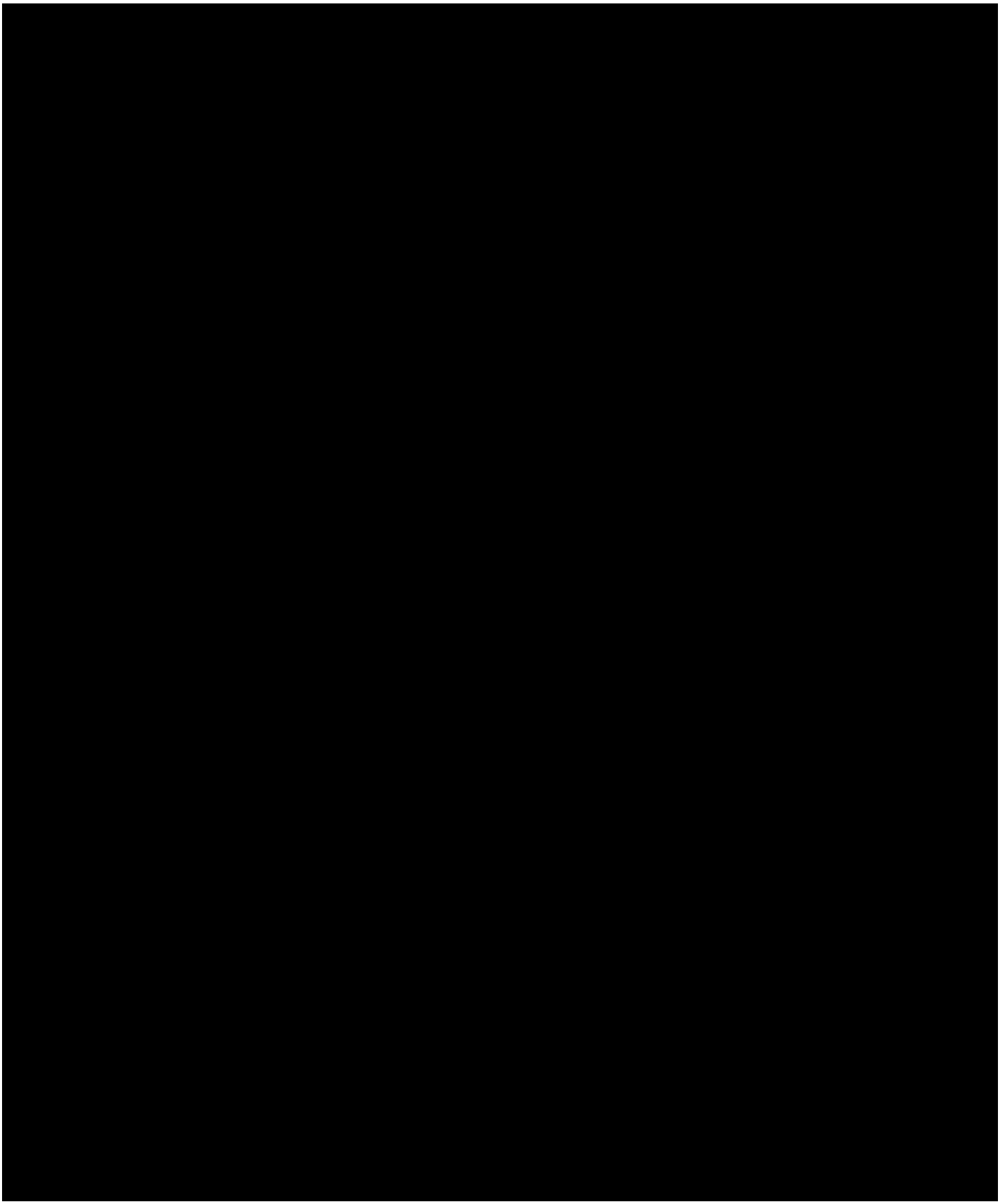
[redacted]

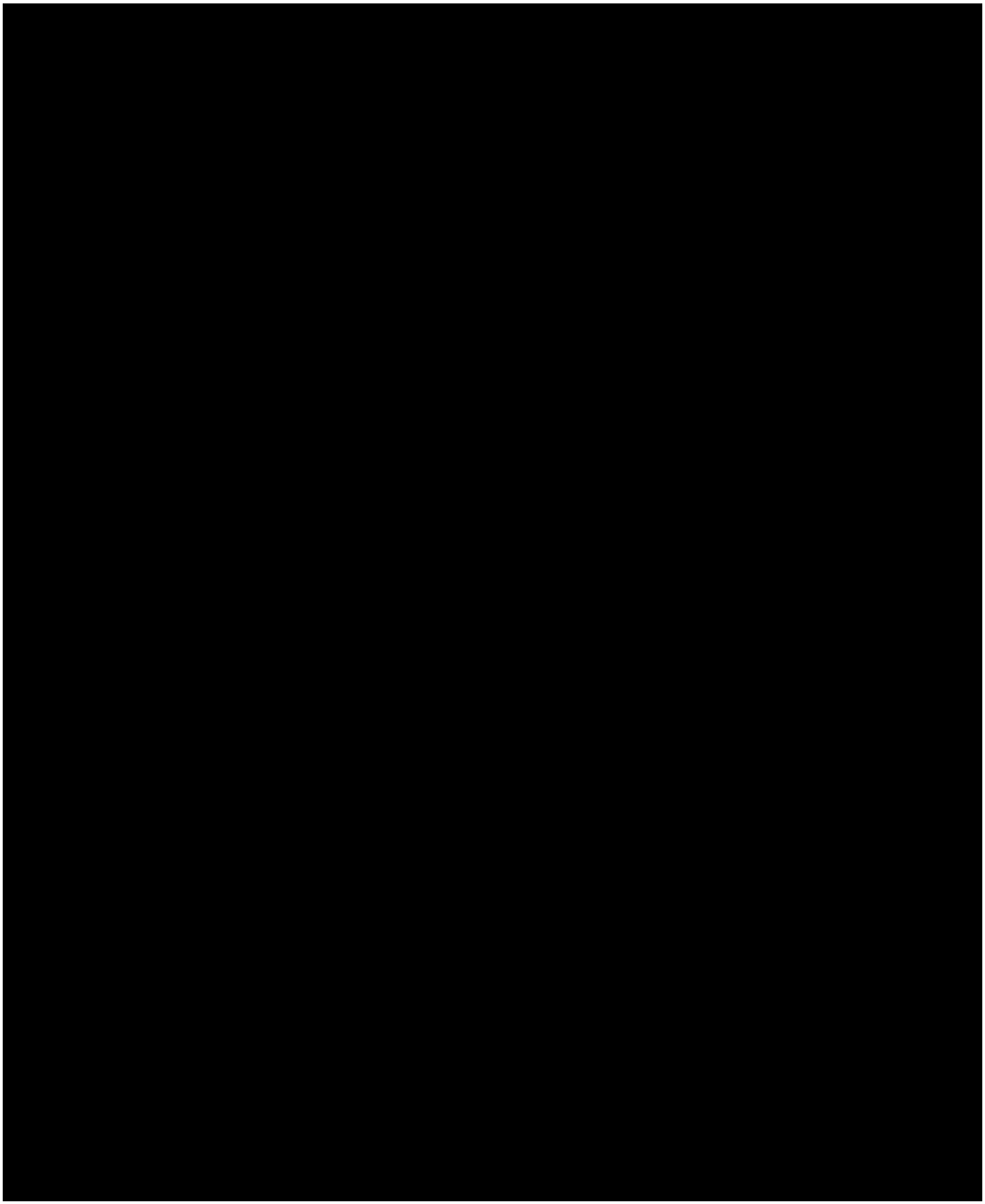
Crown
Commercial

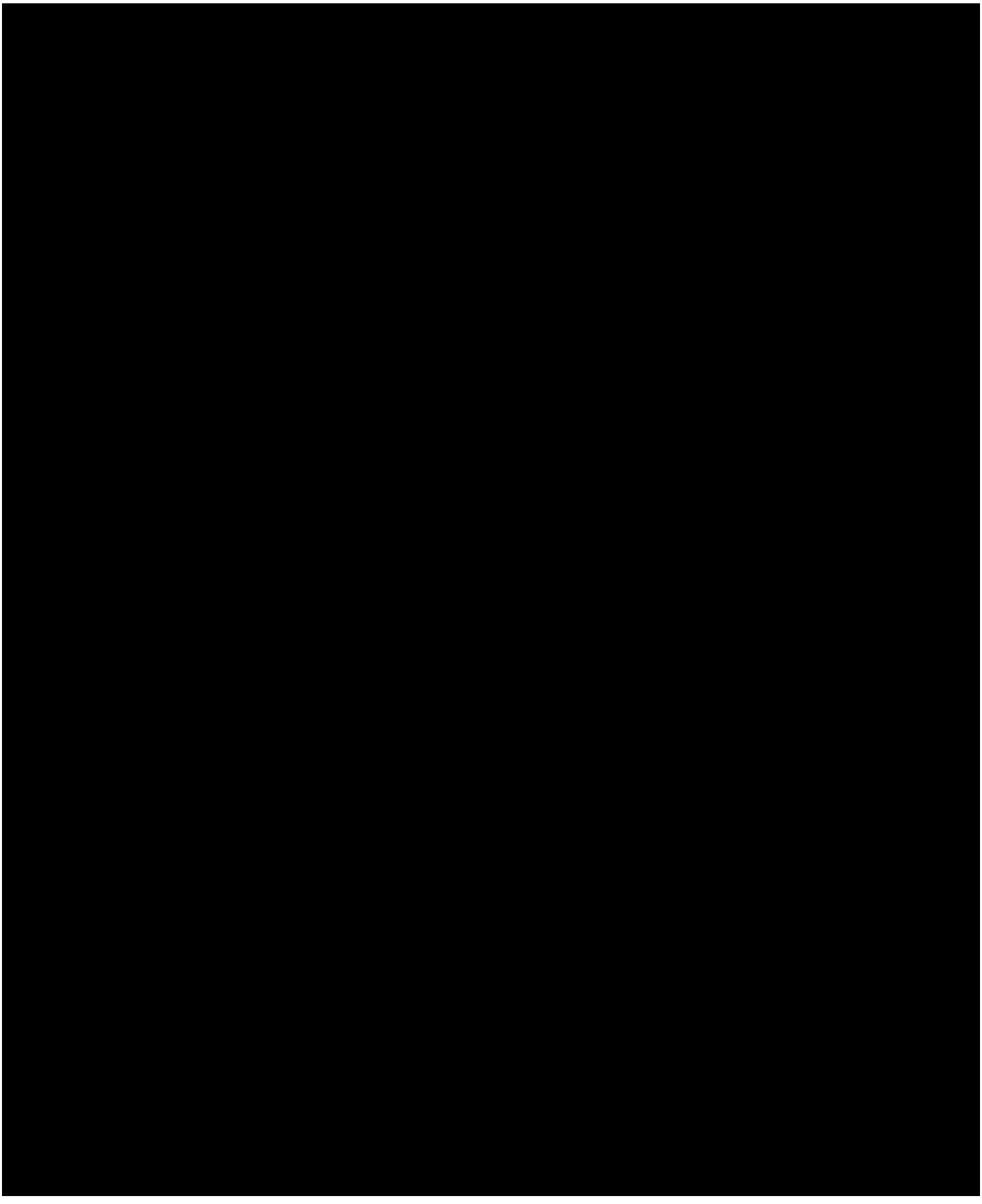
[redacted]



Crown
Commercial

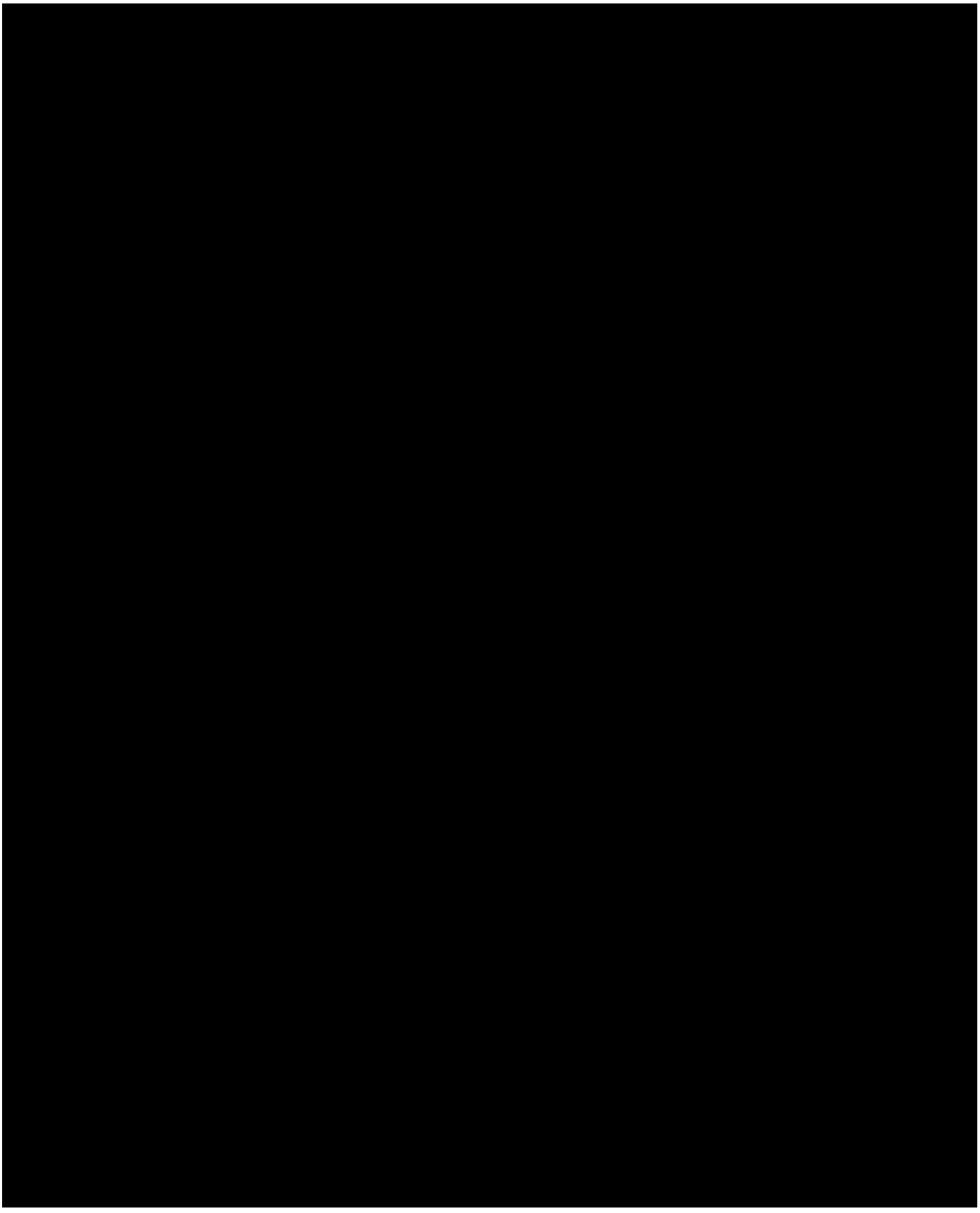


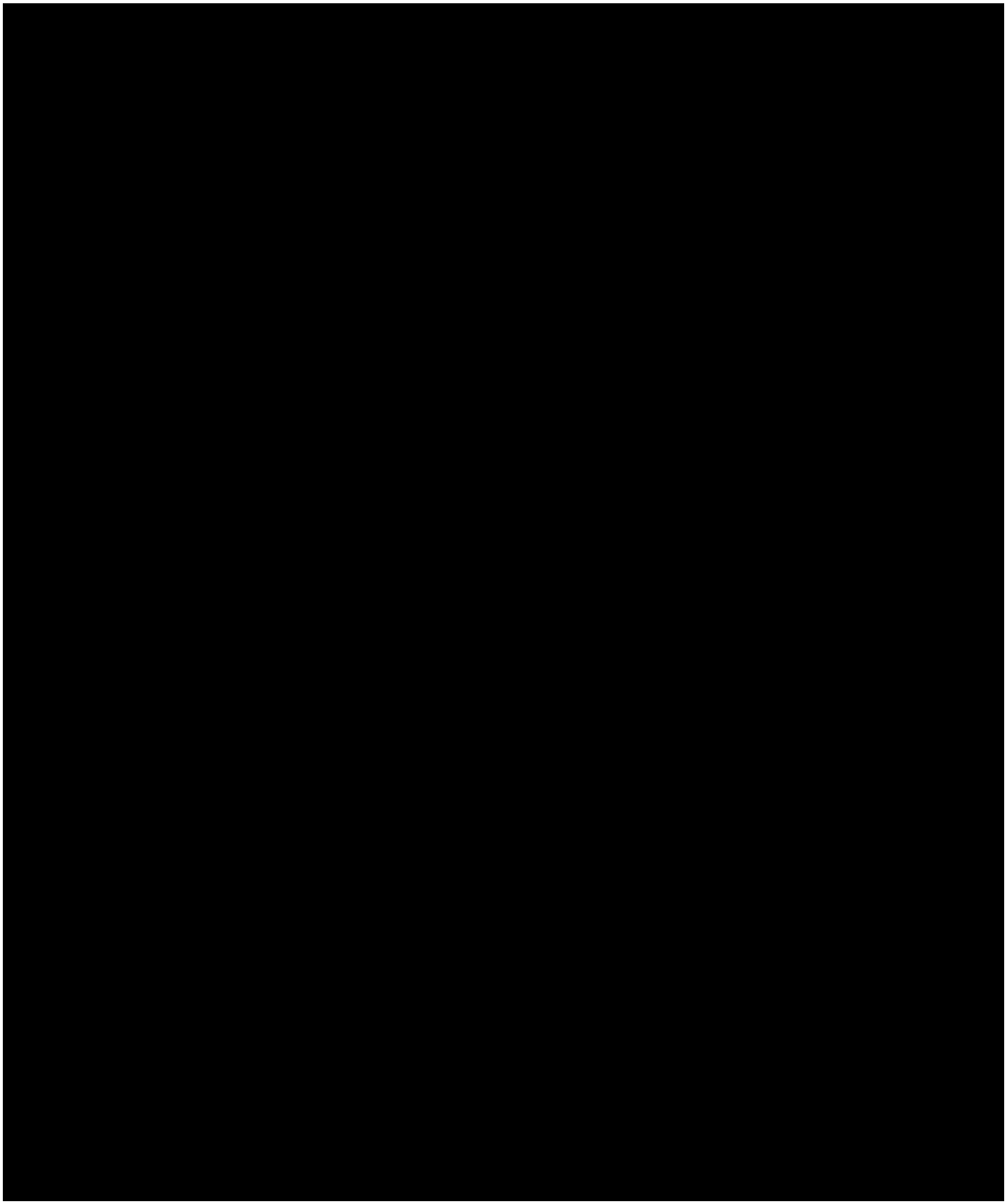


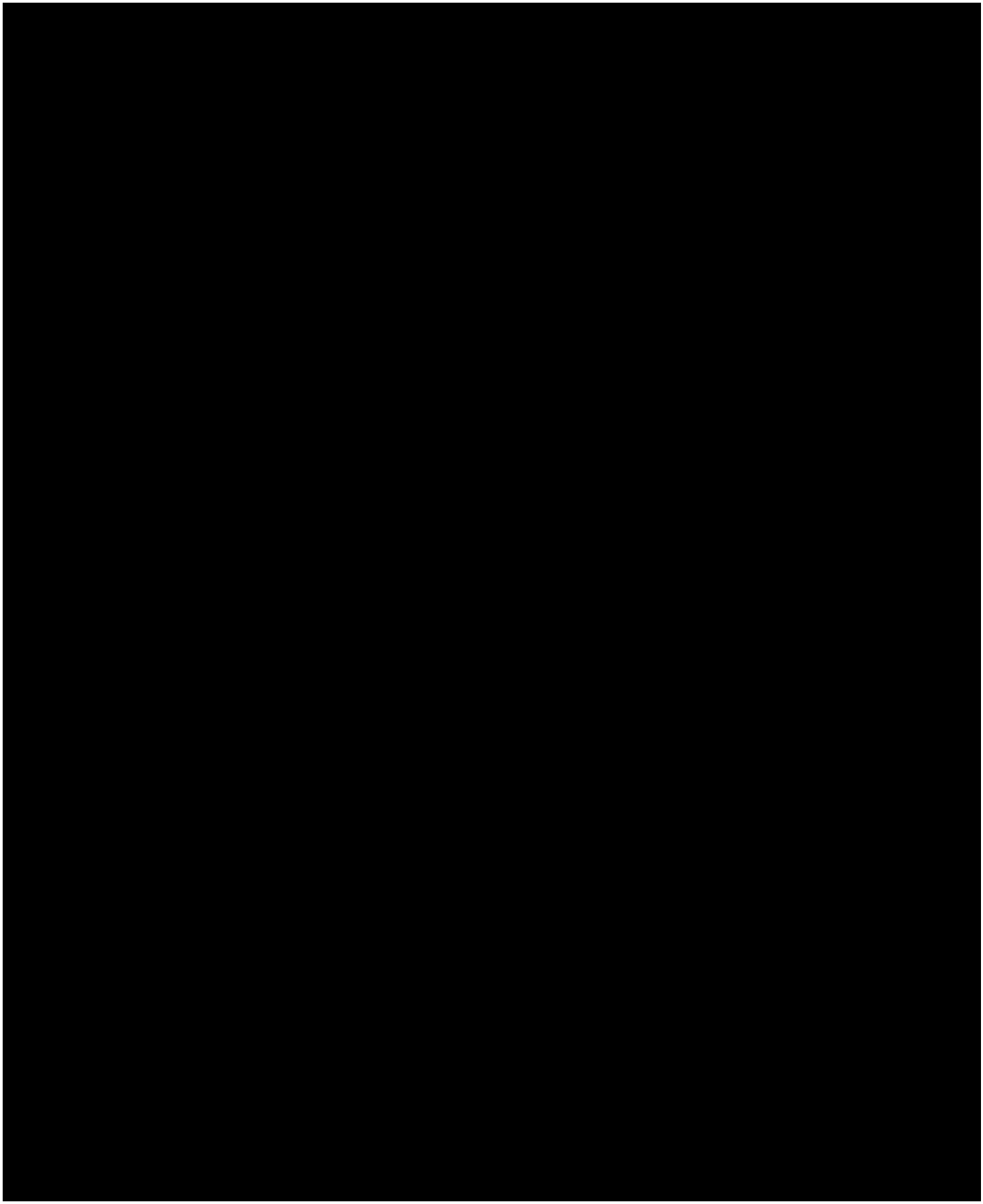


Crown
Commercial

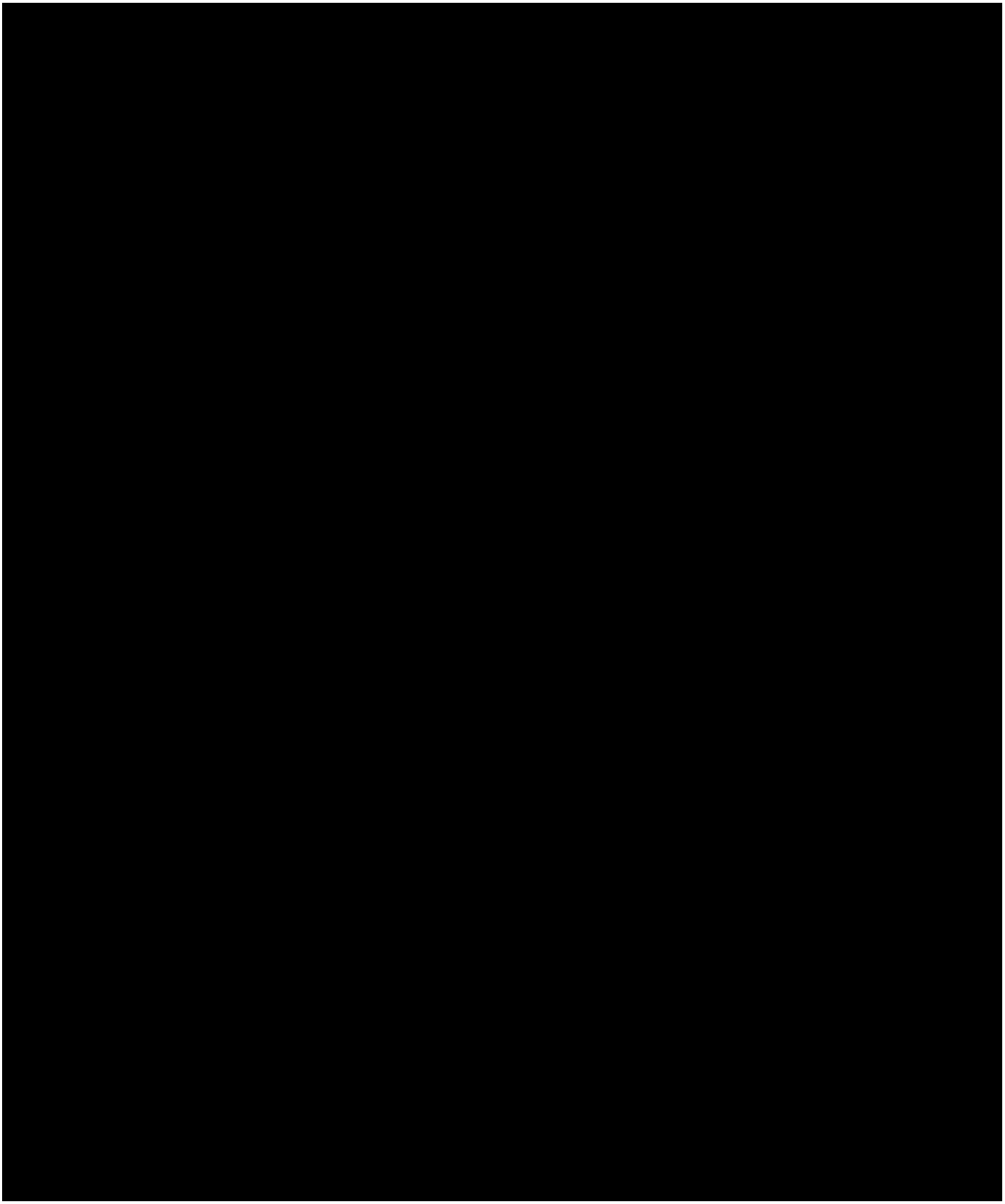
[redacted]





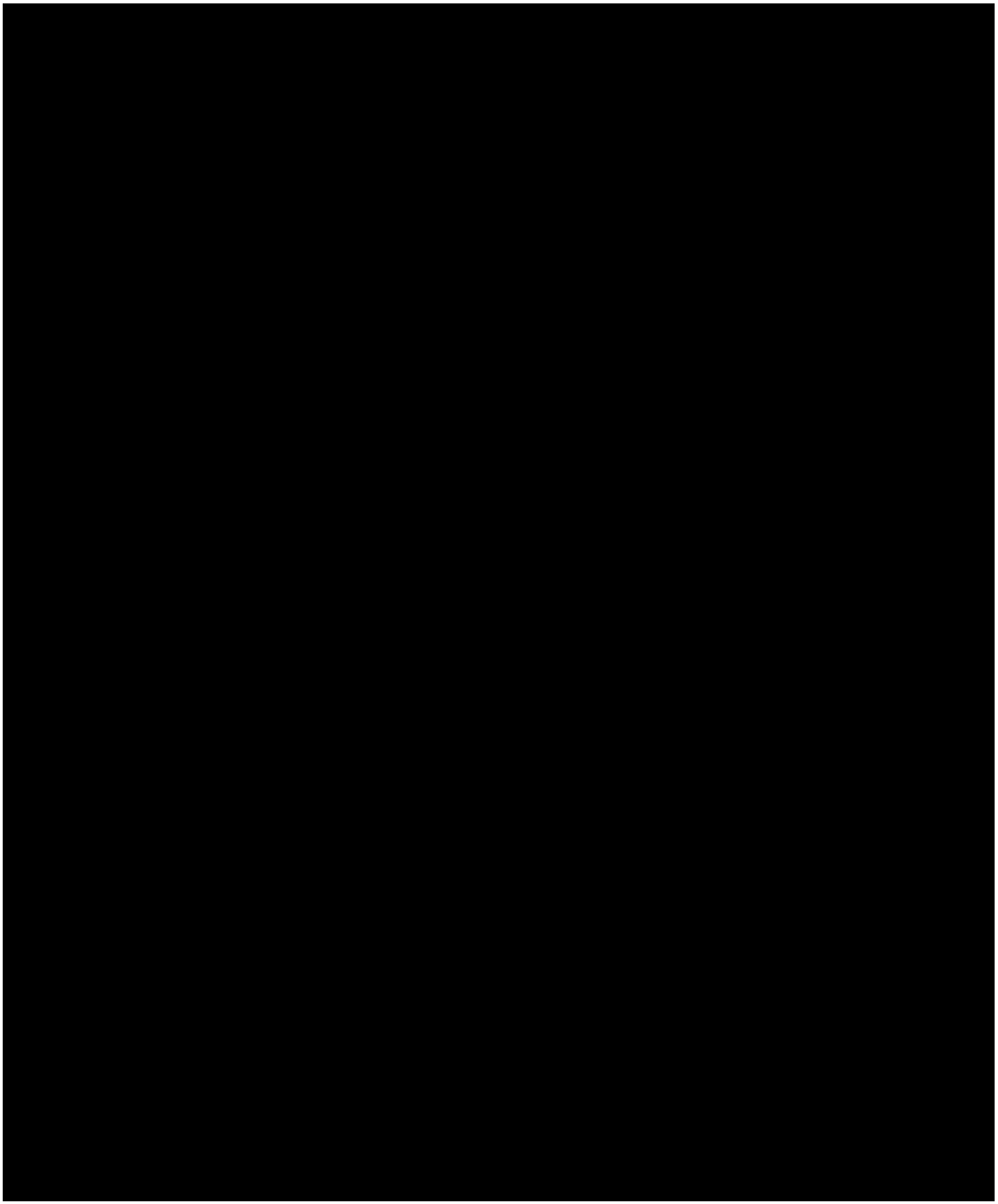


Crown Commercial

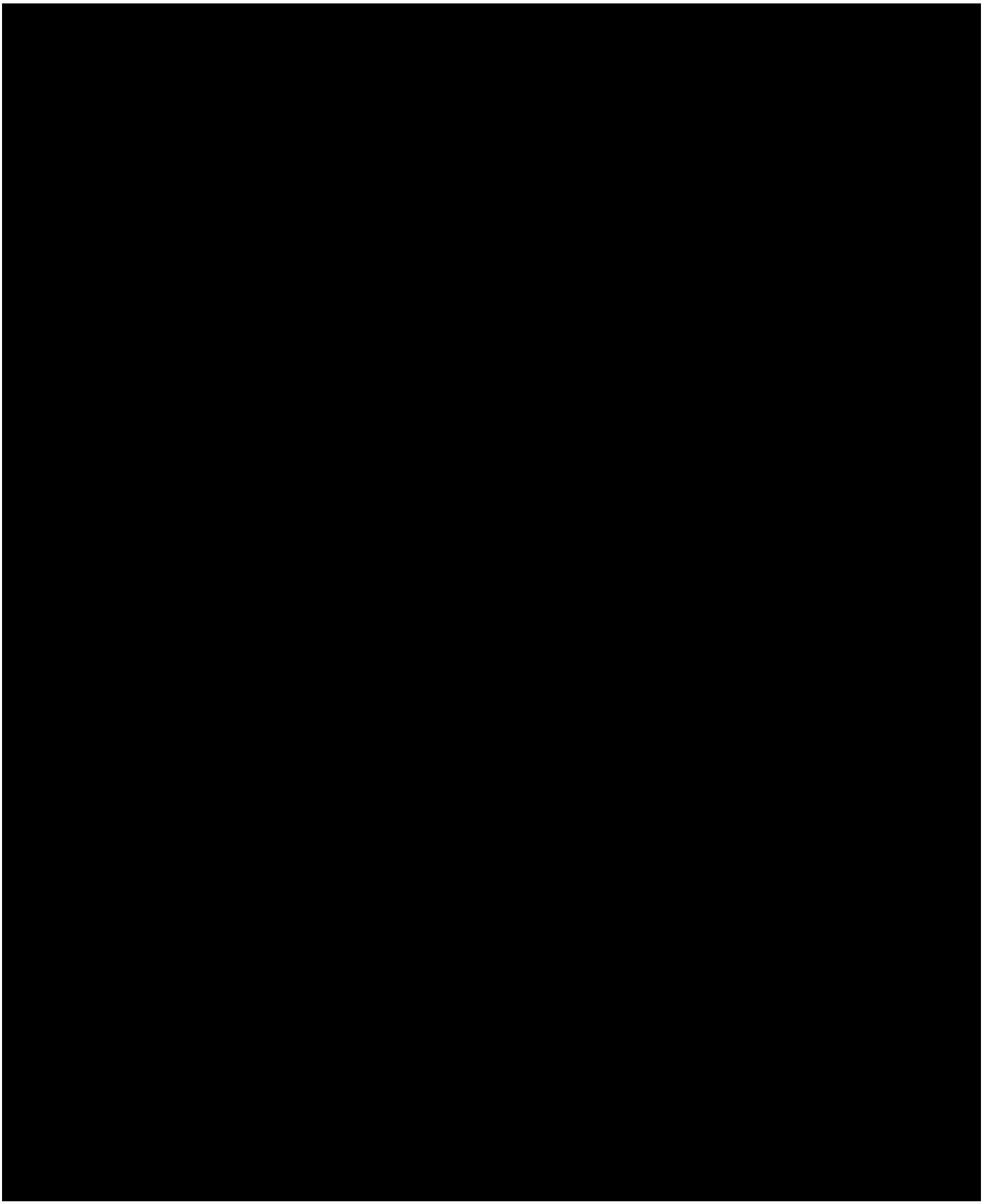


Crown
Commercial

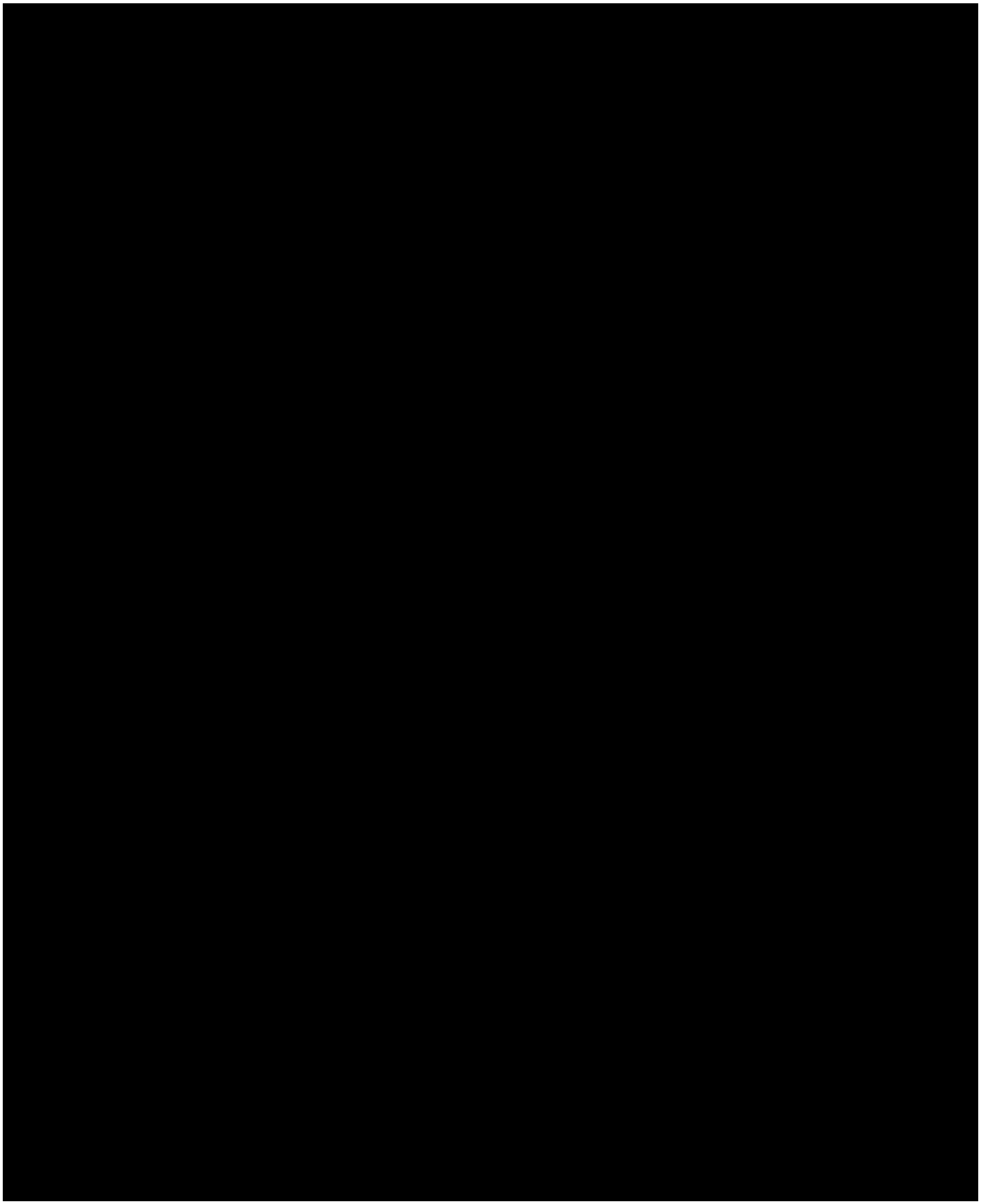
[redacted]

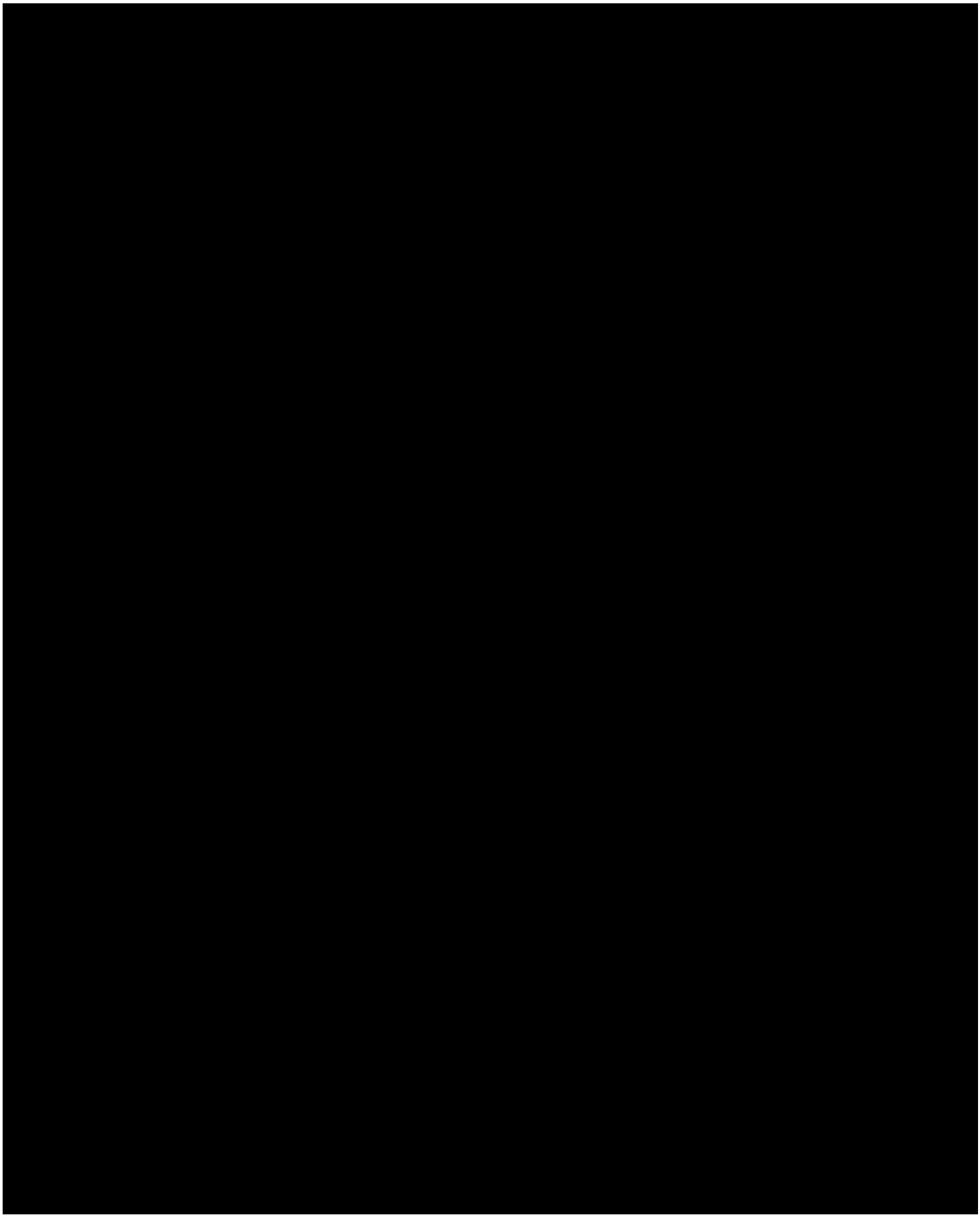


Crown
Commercial



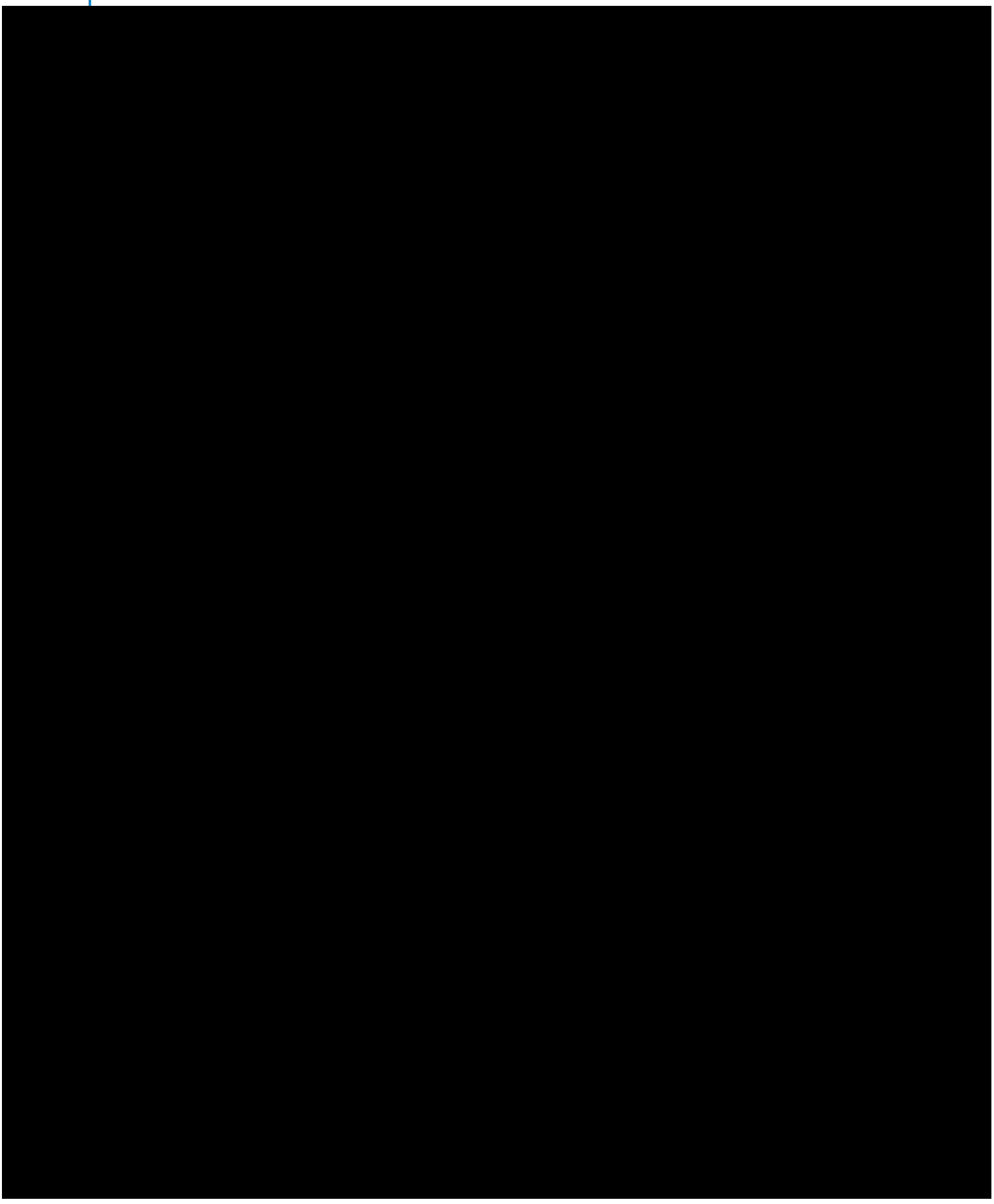
[redacted]





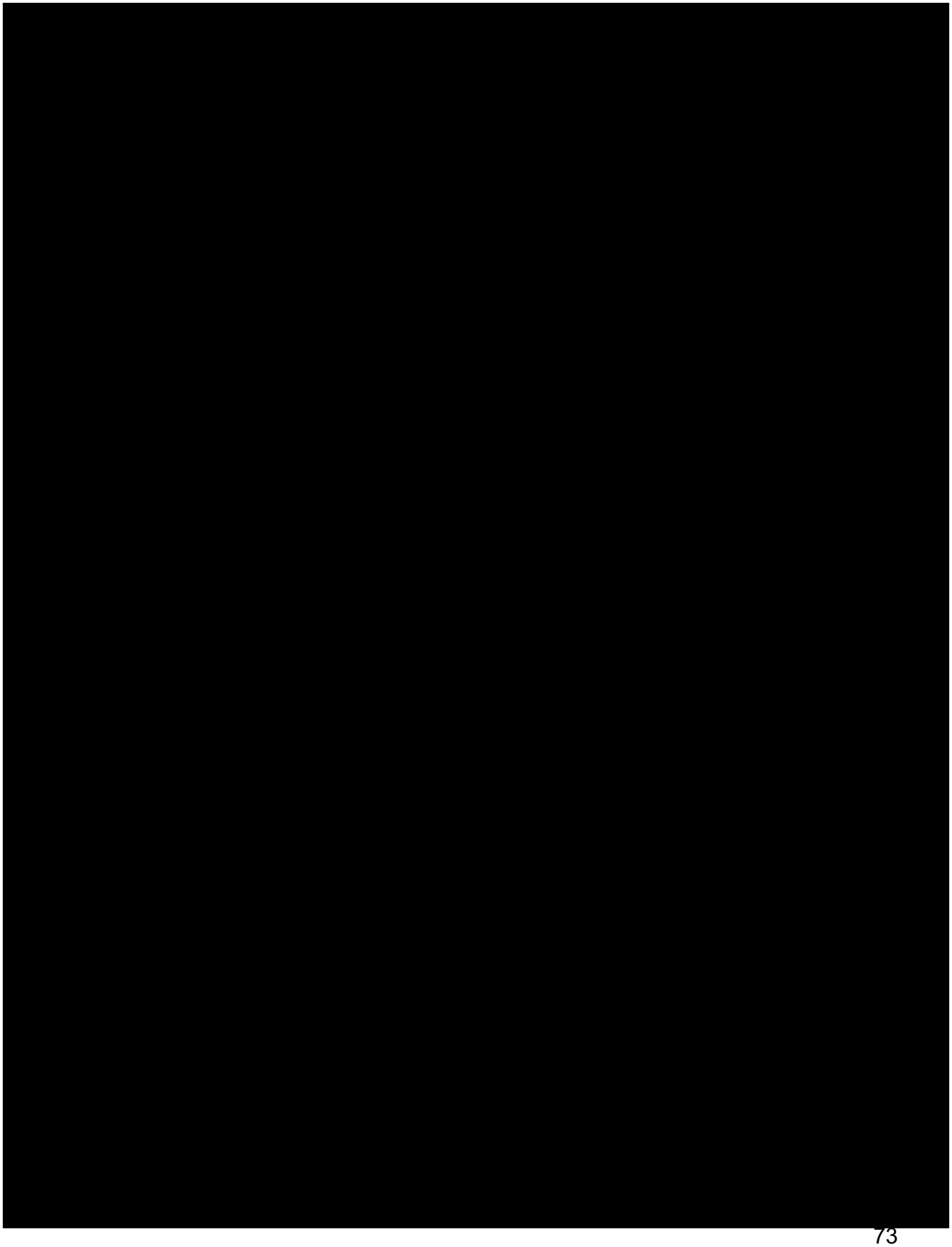
Crown
Commercial

[redacted]

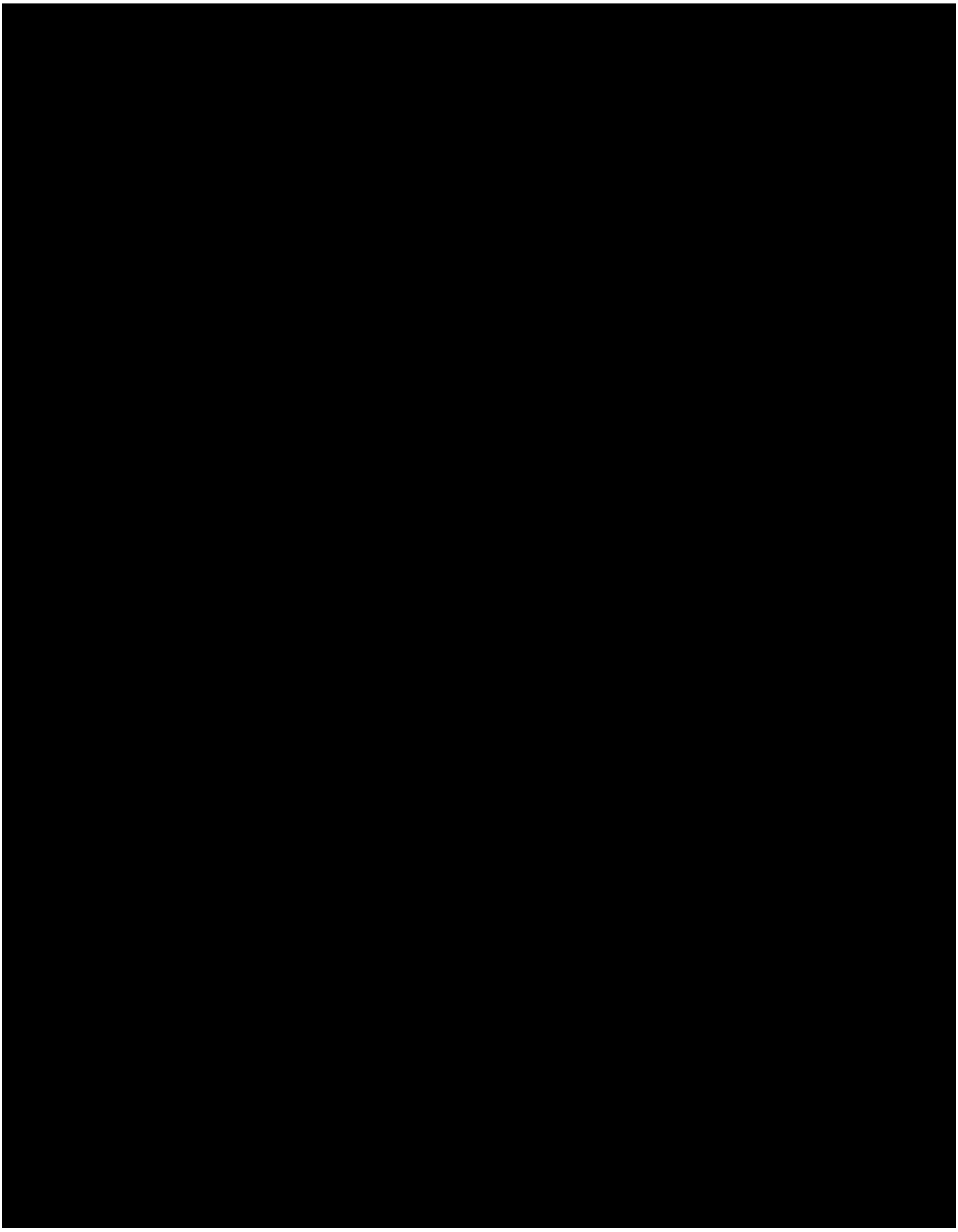


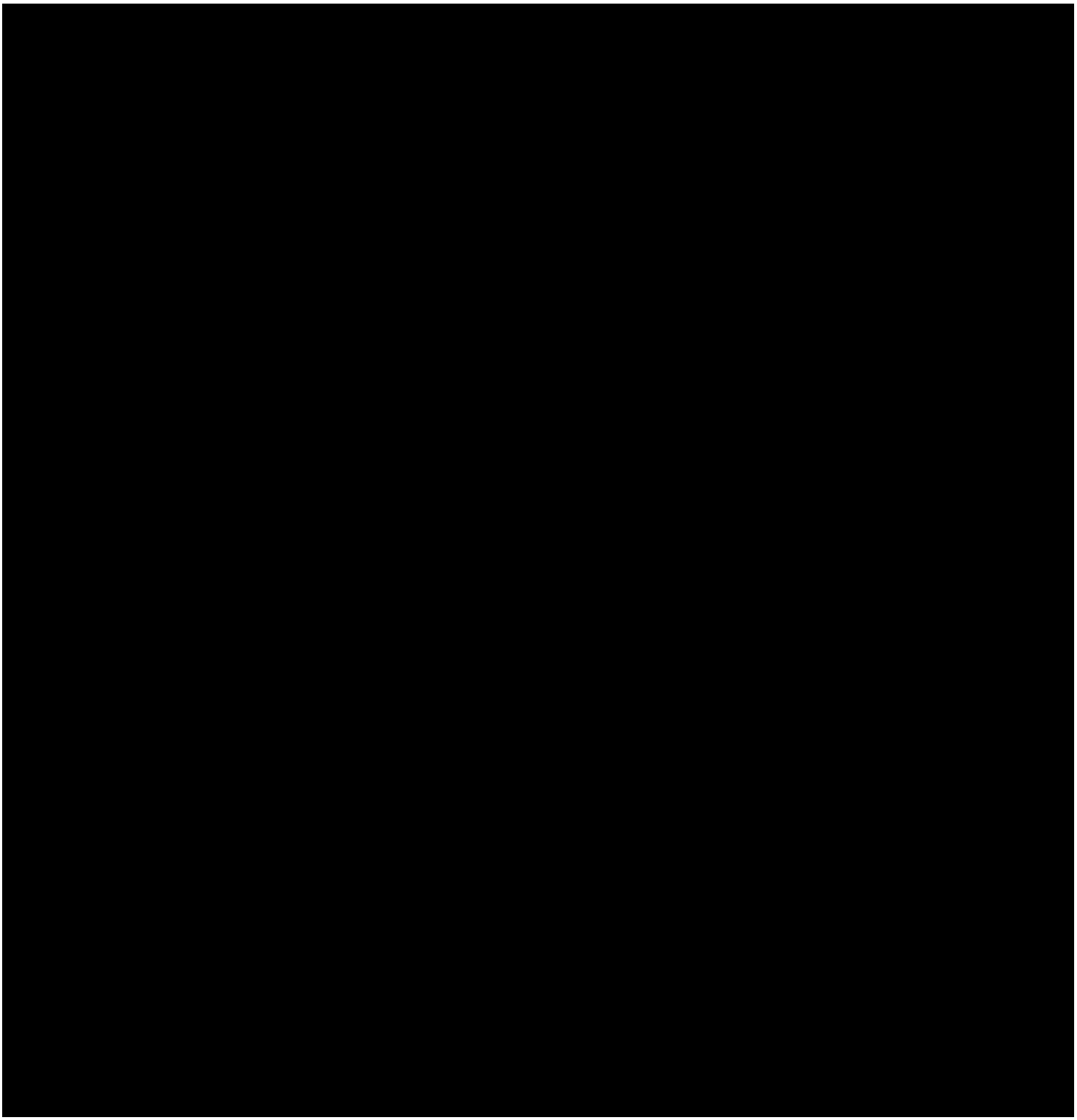
Crown
Commercial

[redacted]



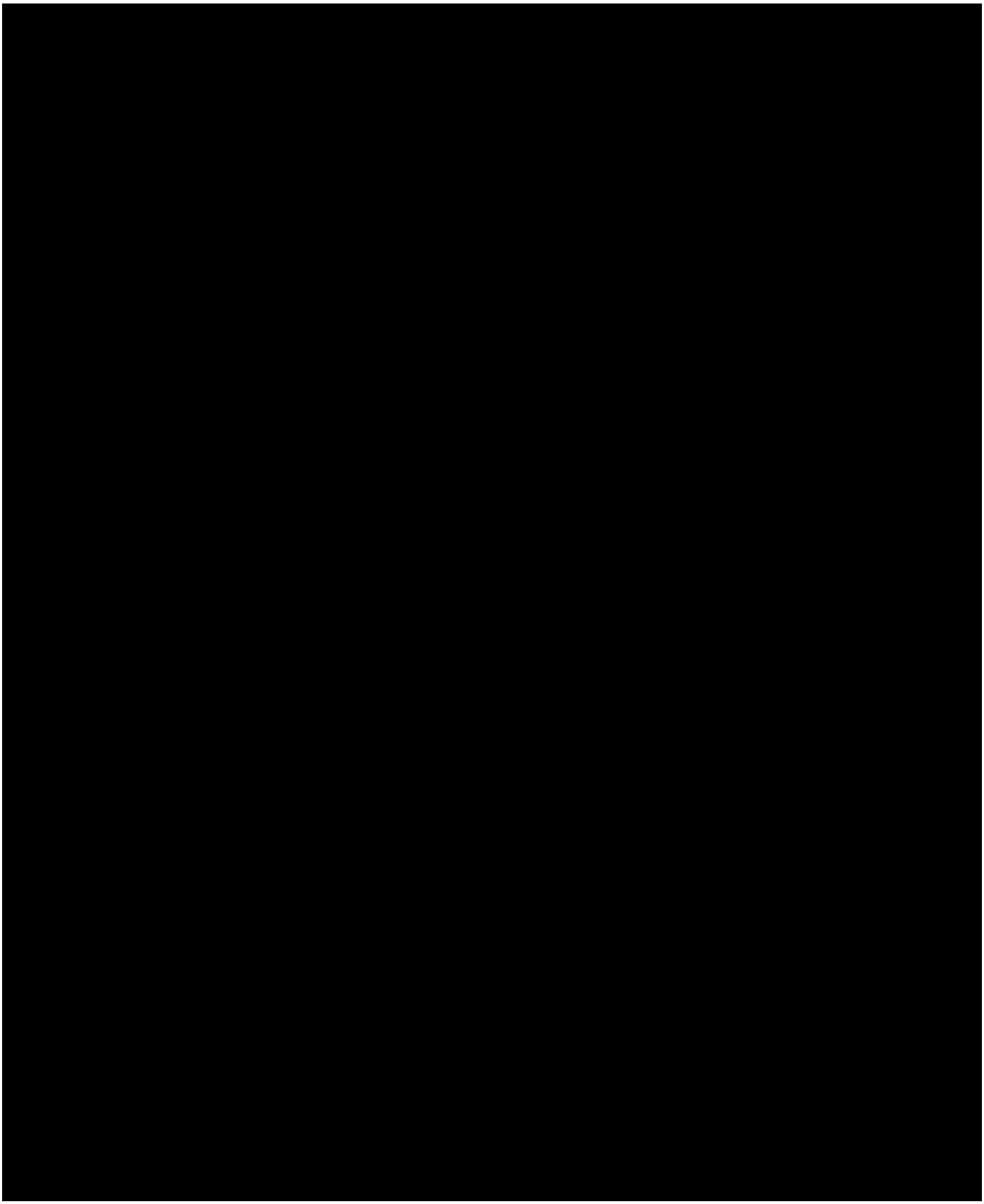
Crown
Commercial

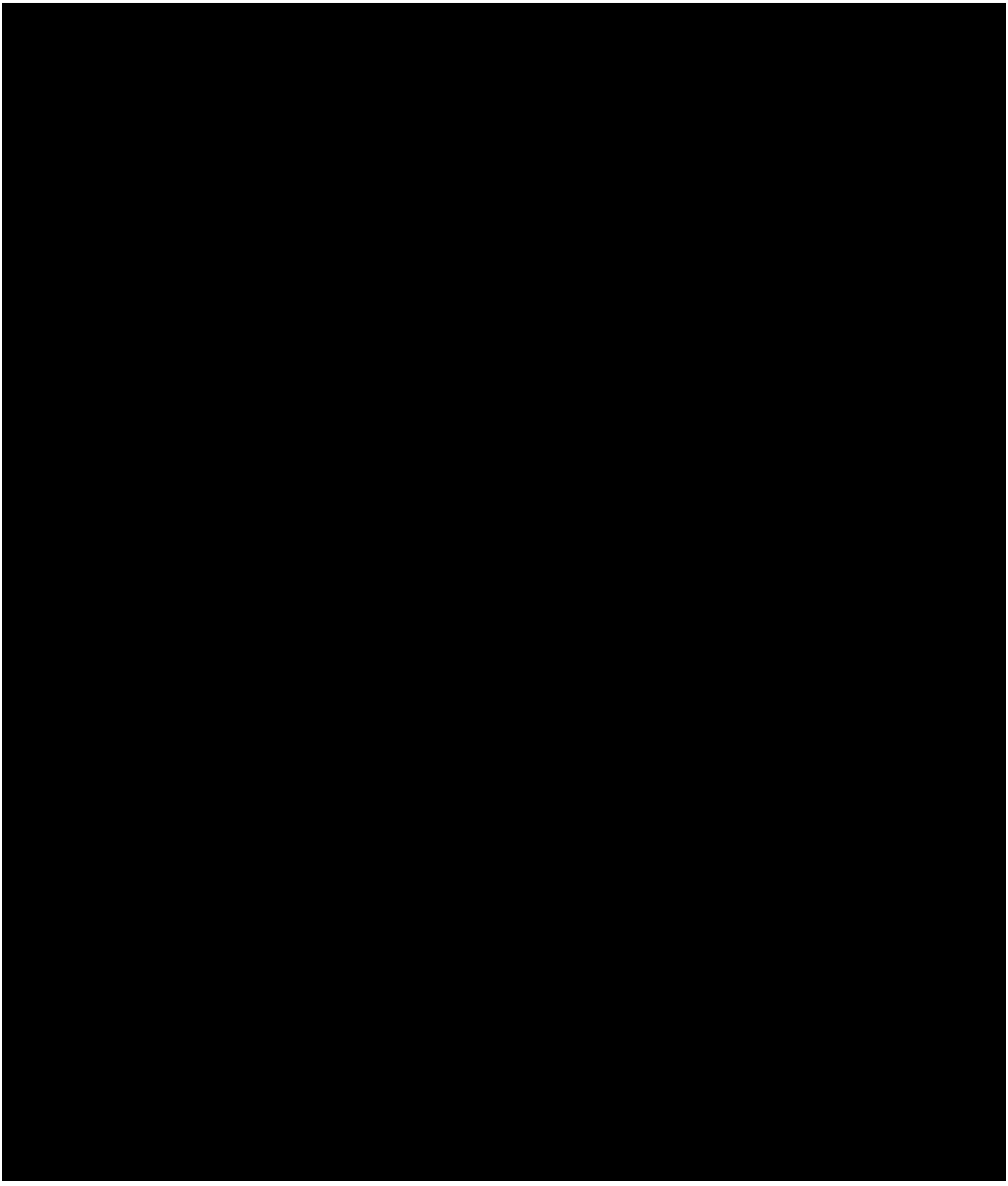


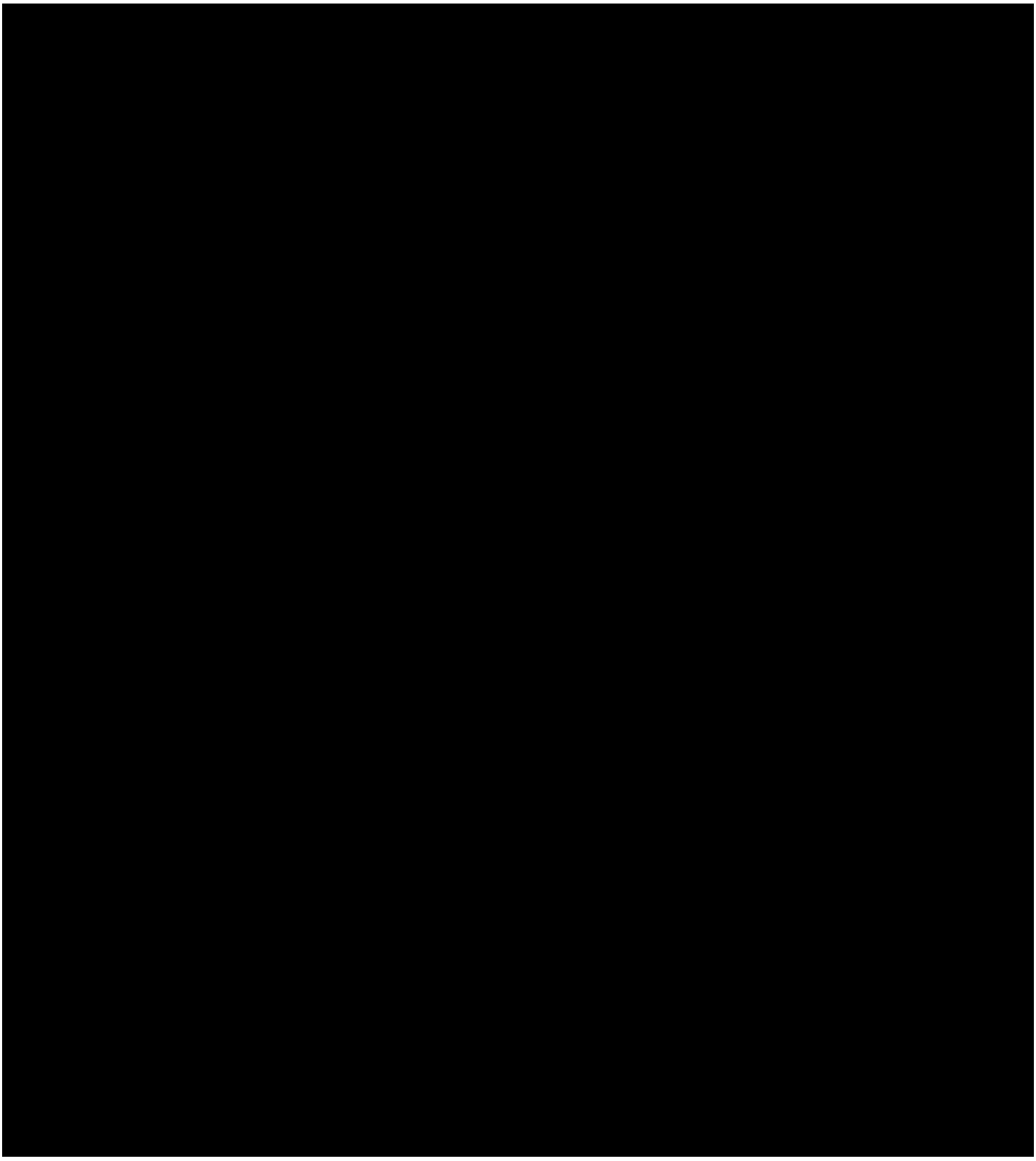


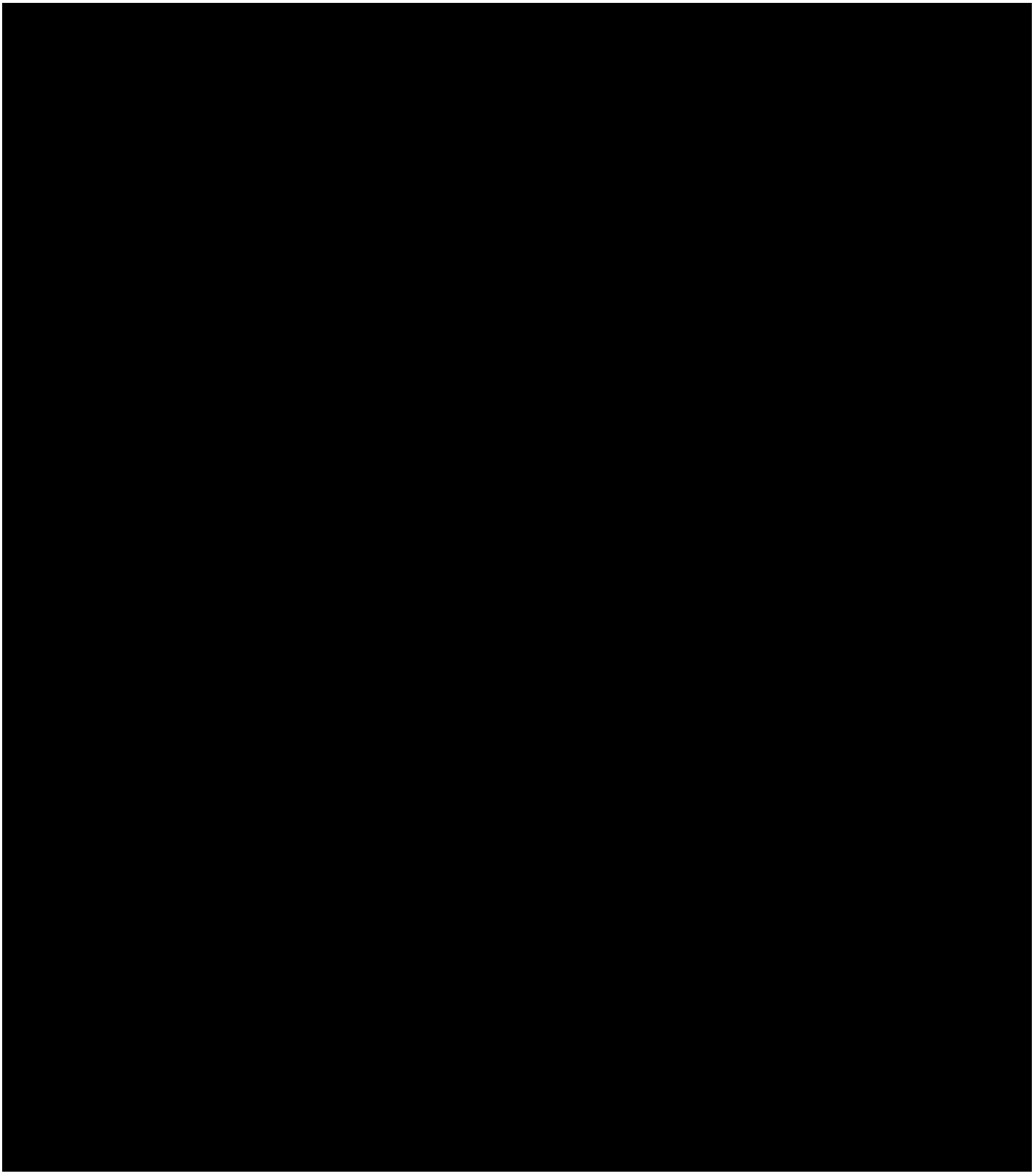
Crown Commercial

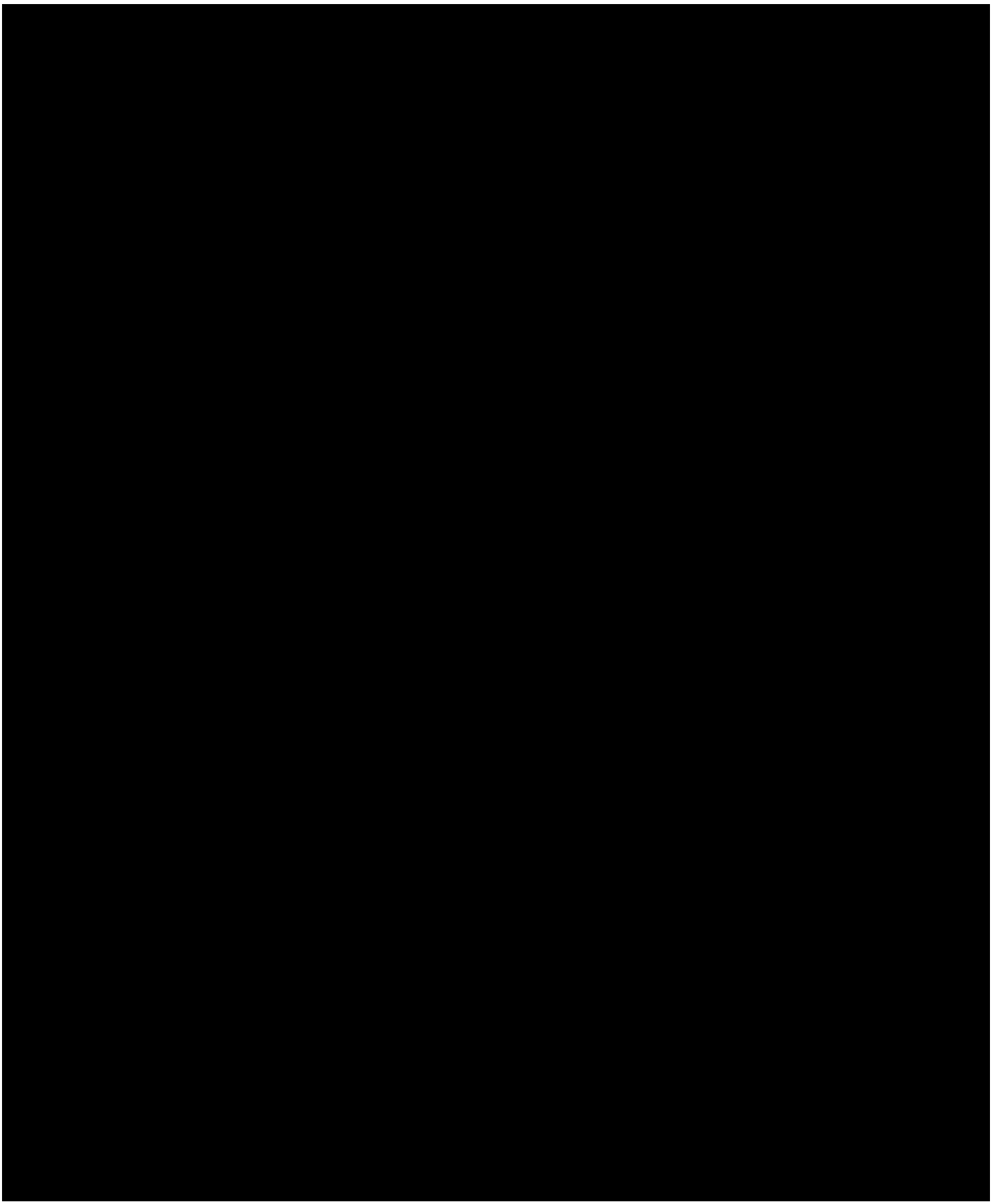
Crown Commercial

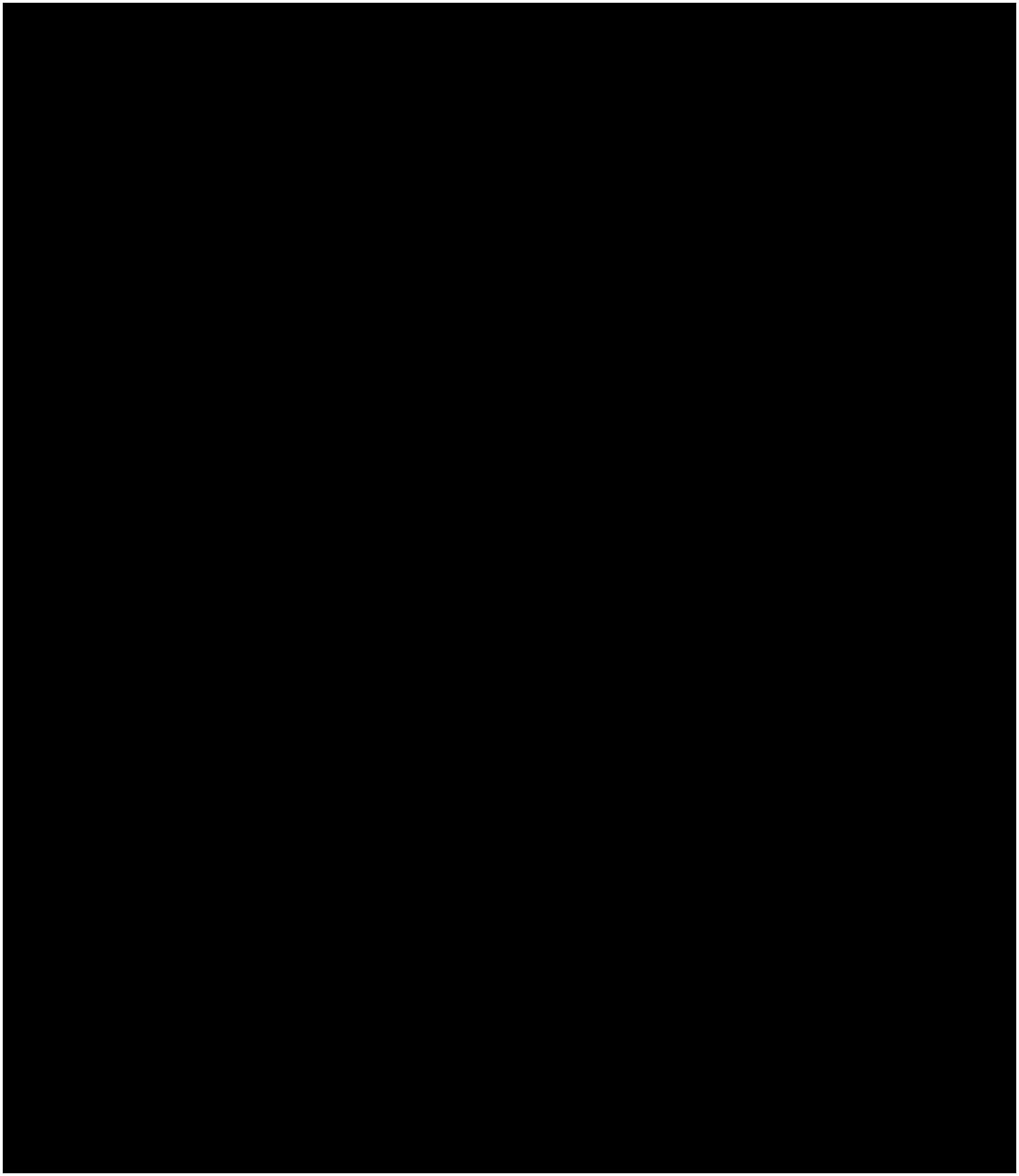






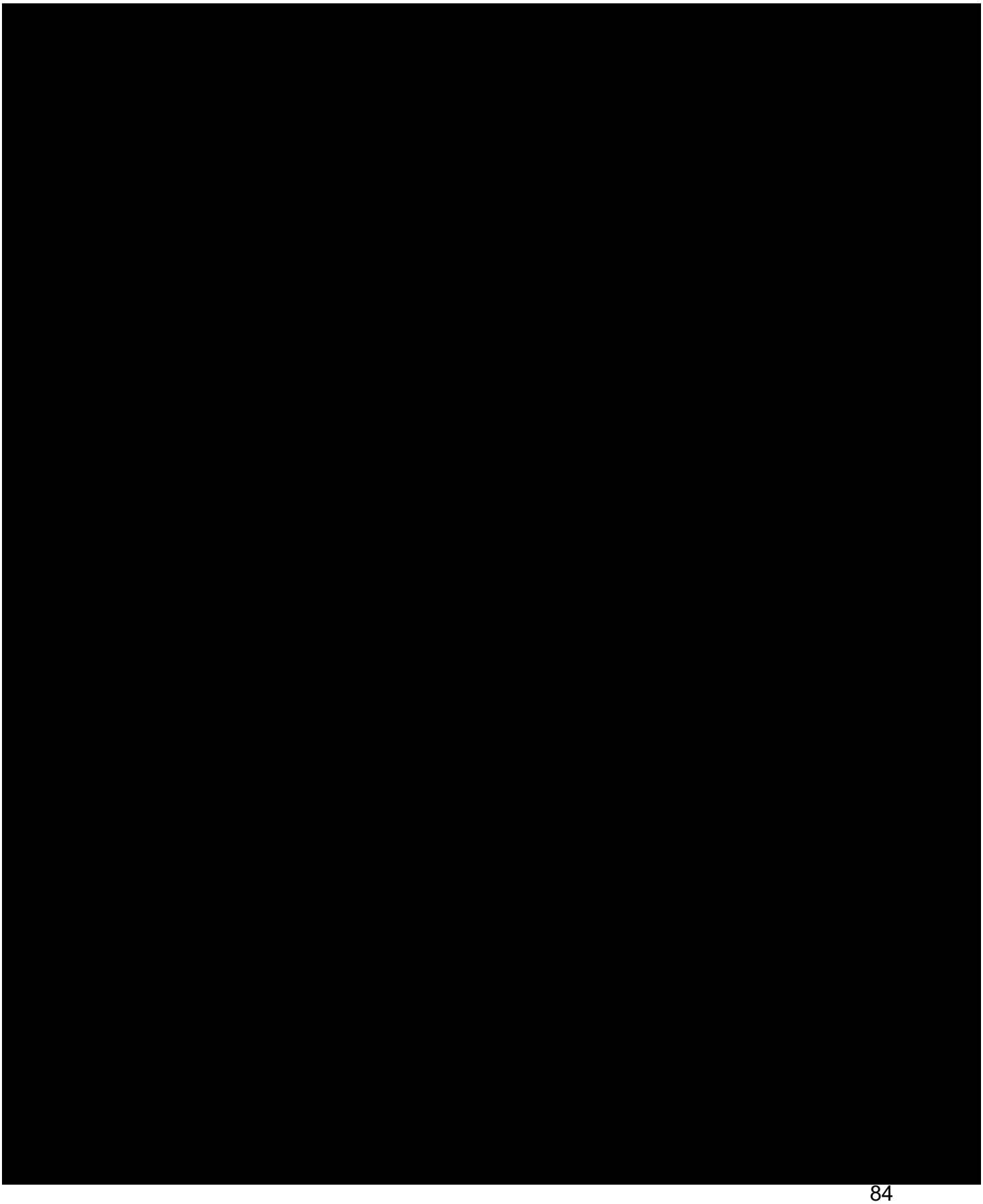


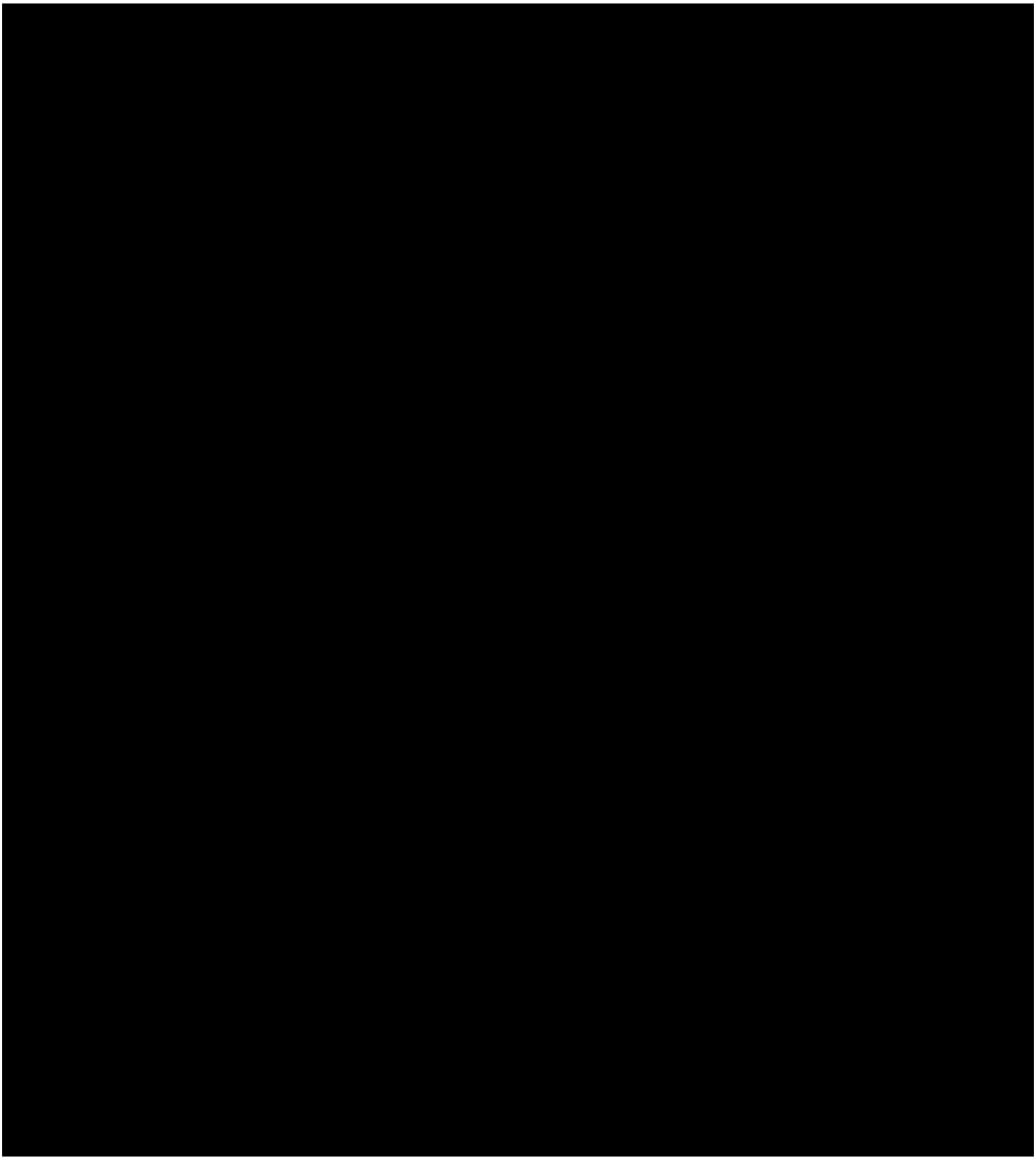


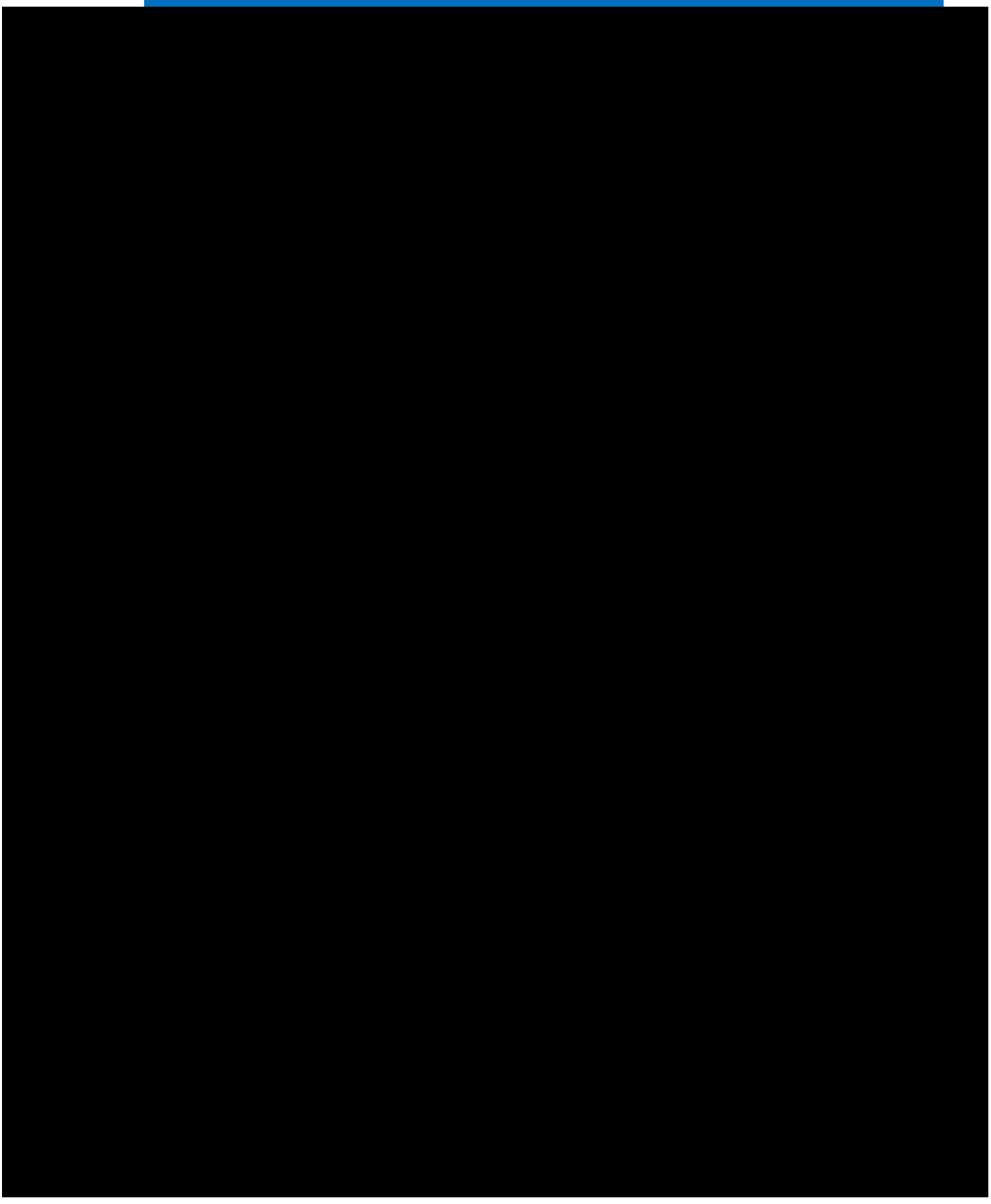


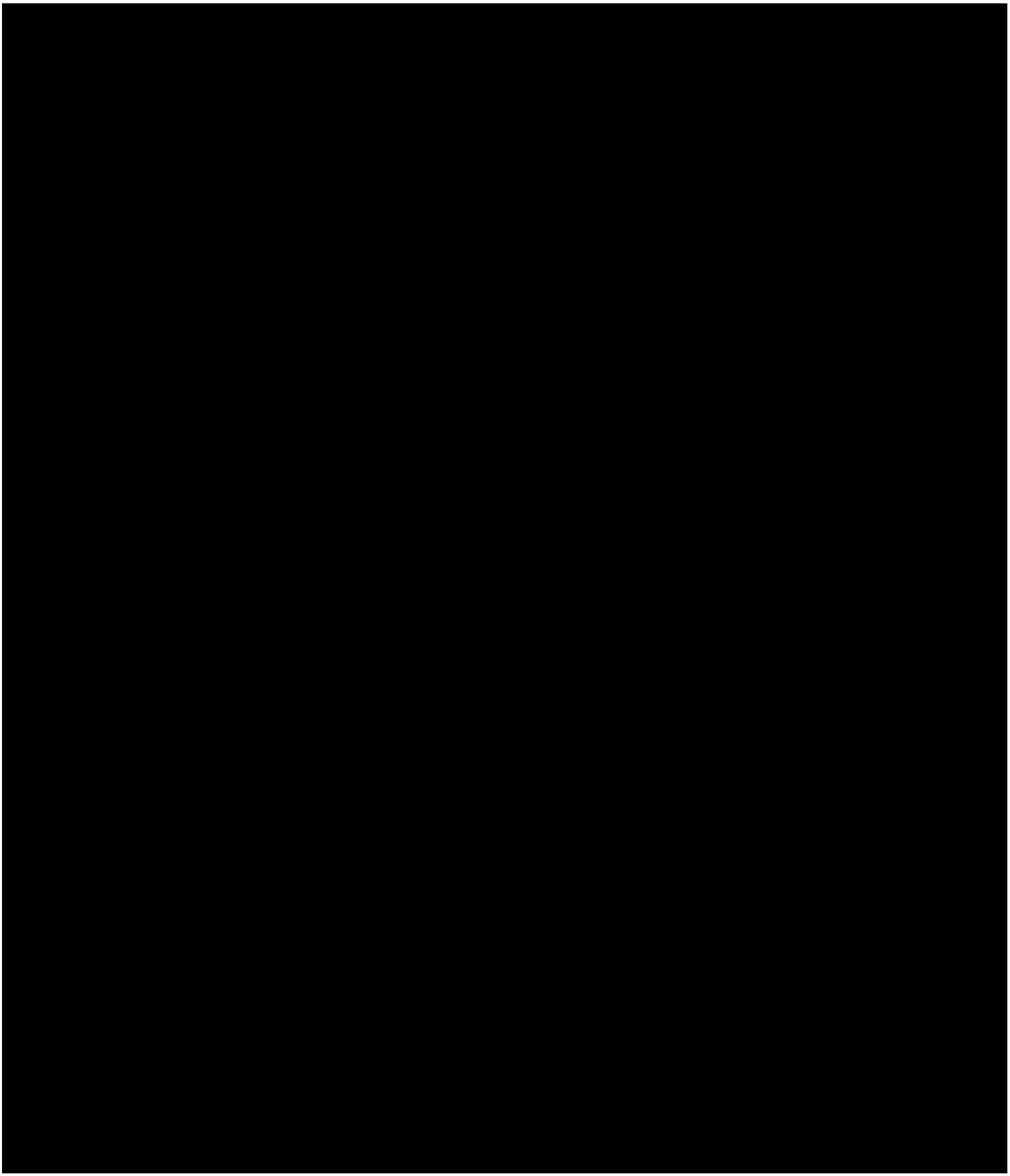
Crown
Commercial

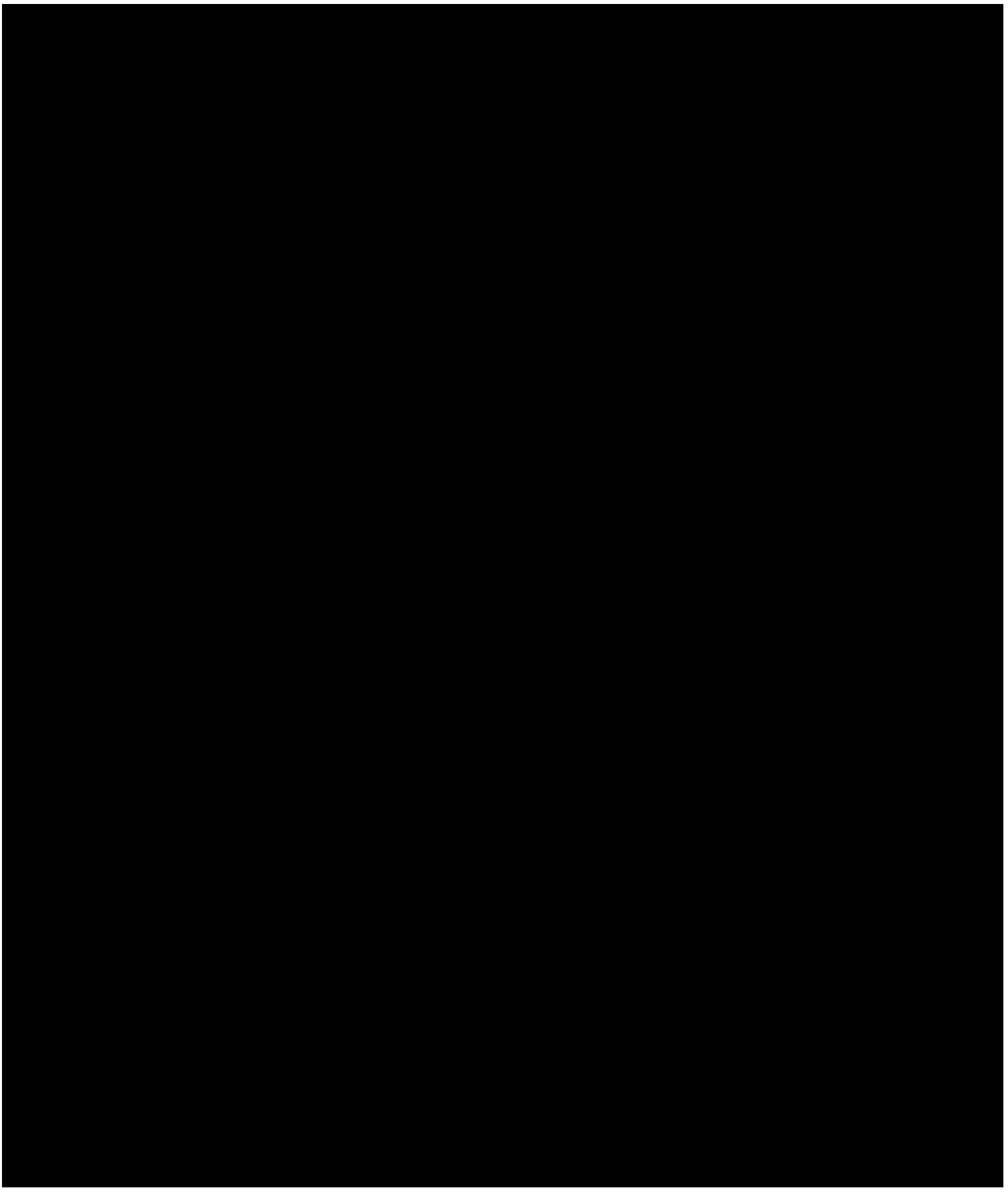
[redacted]

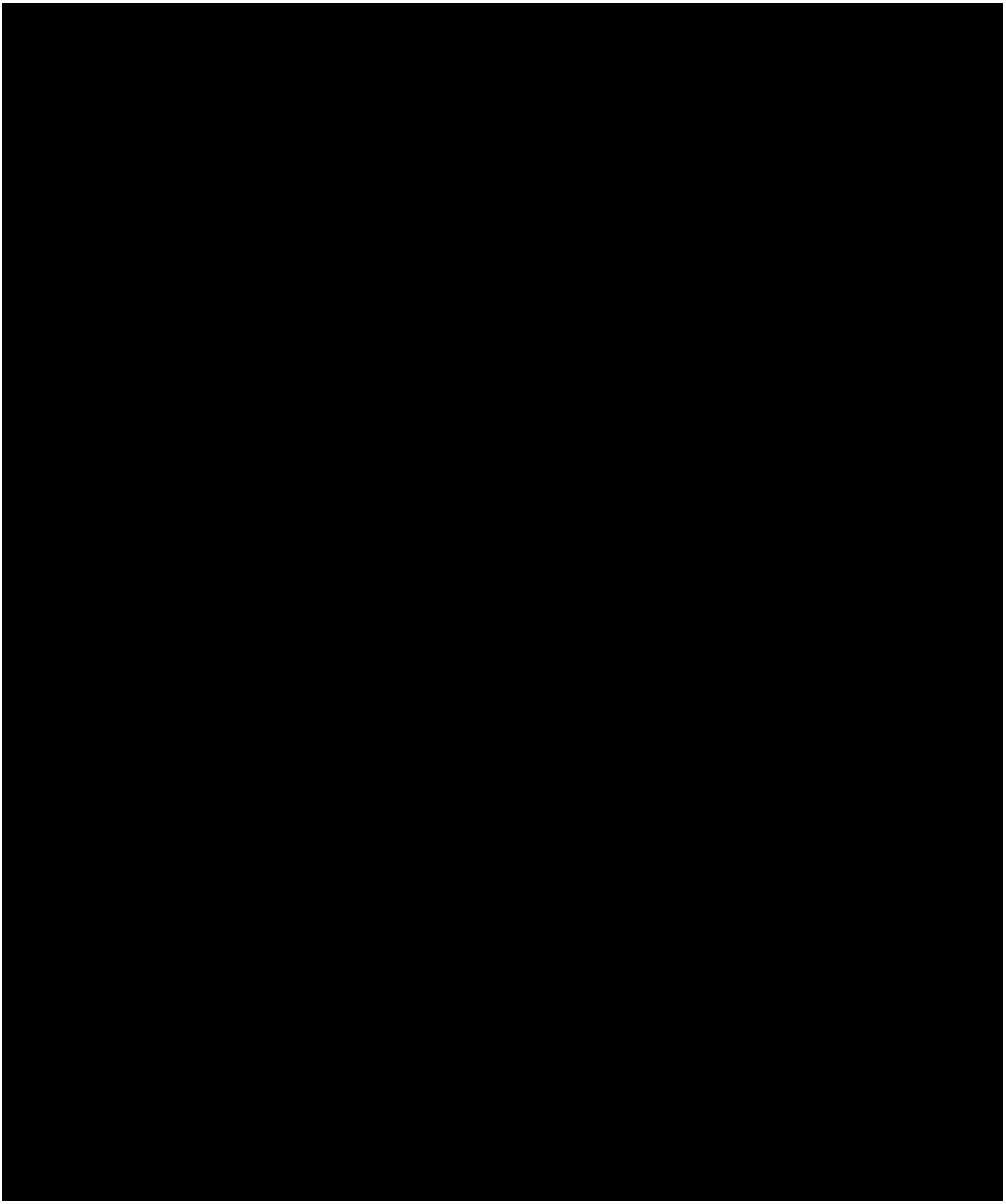


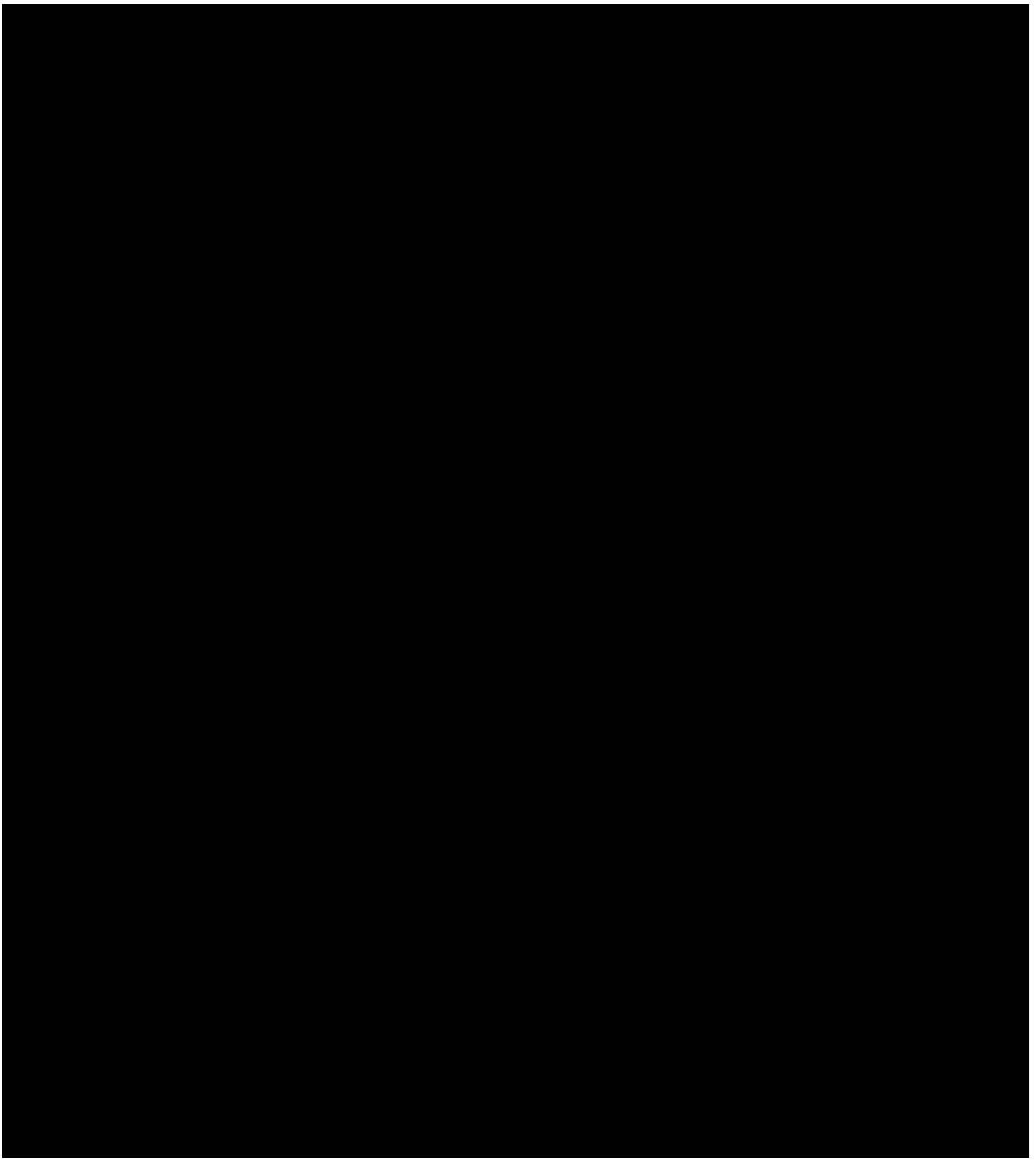


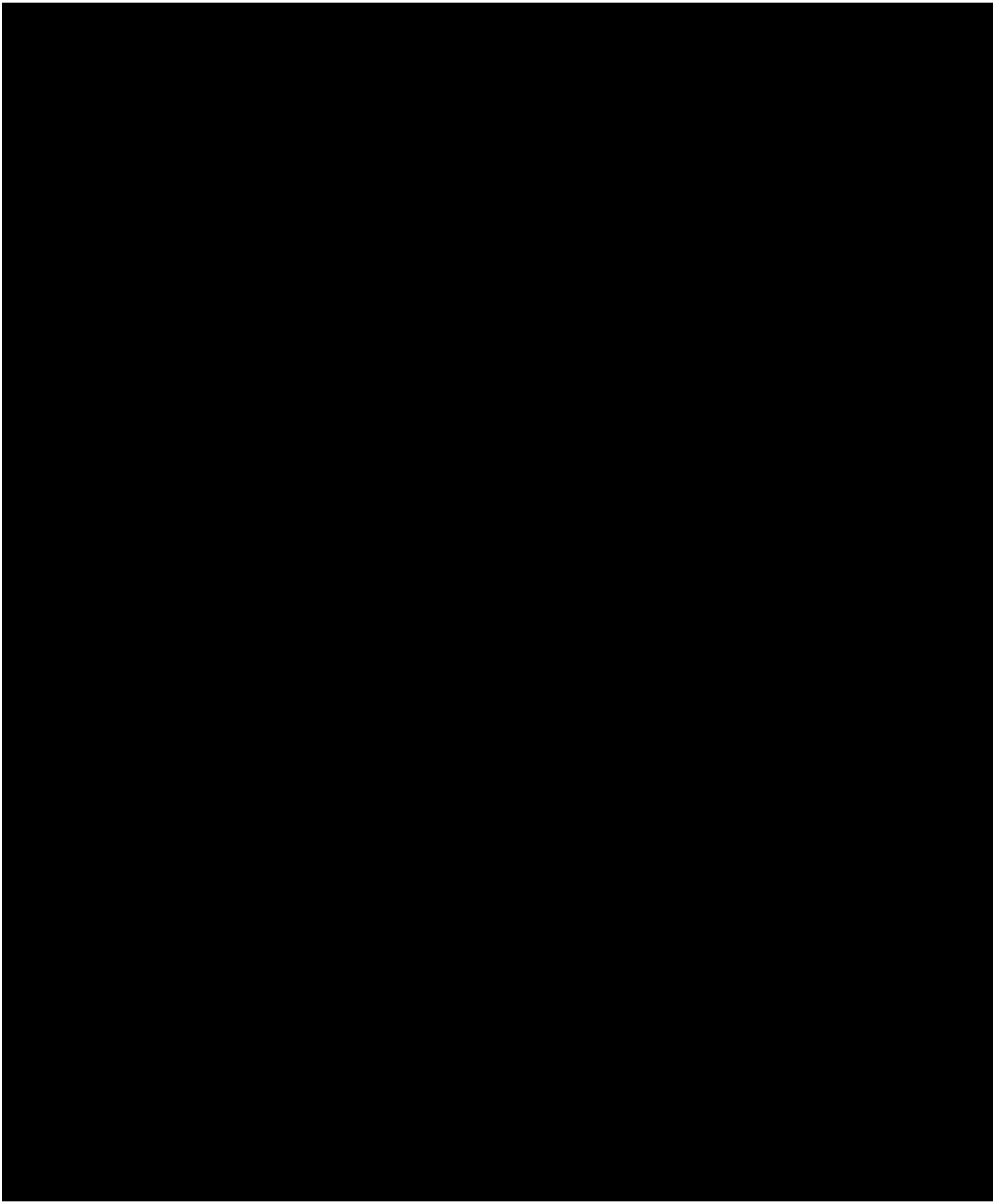


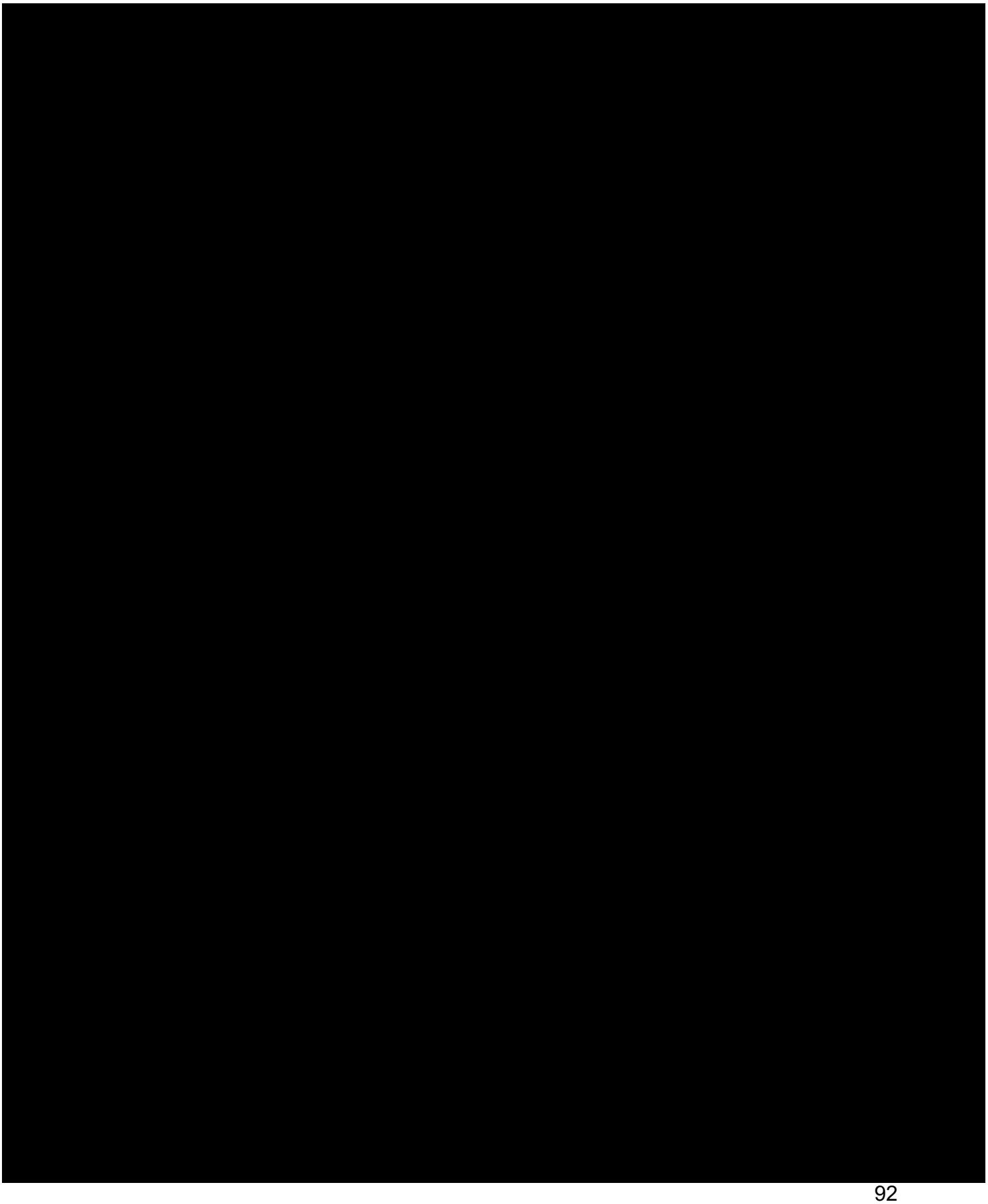


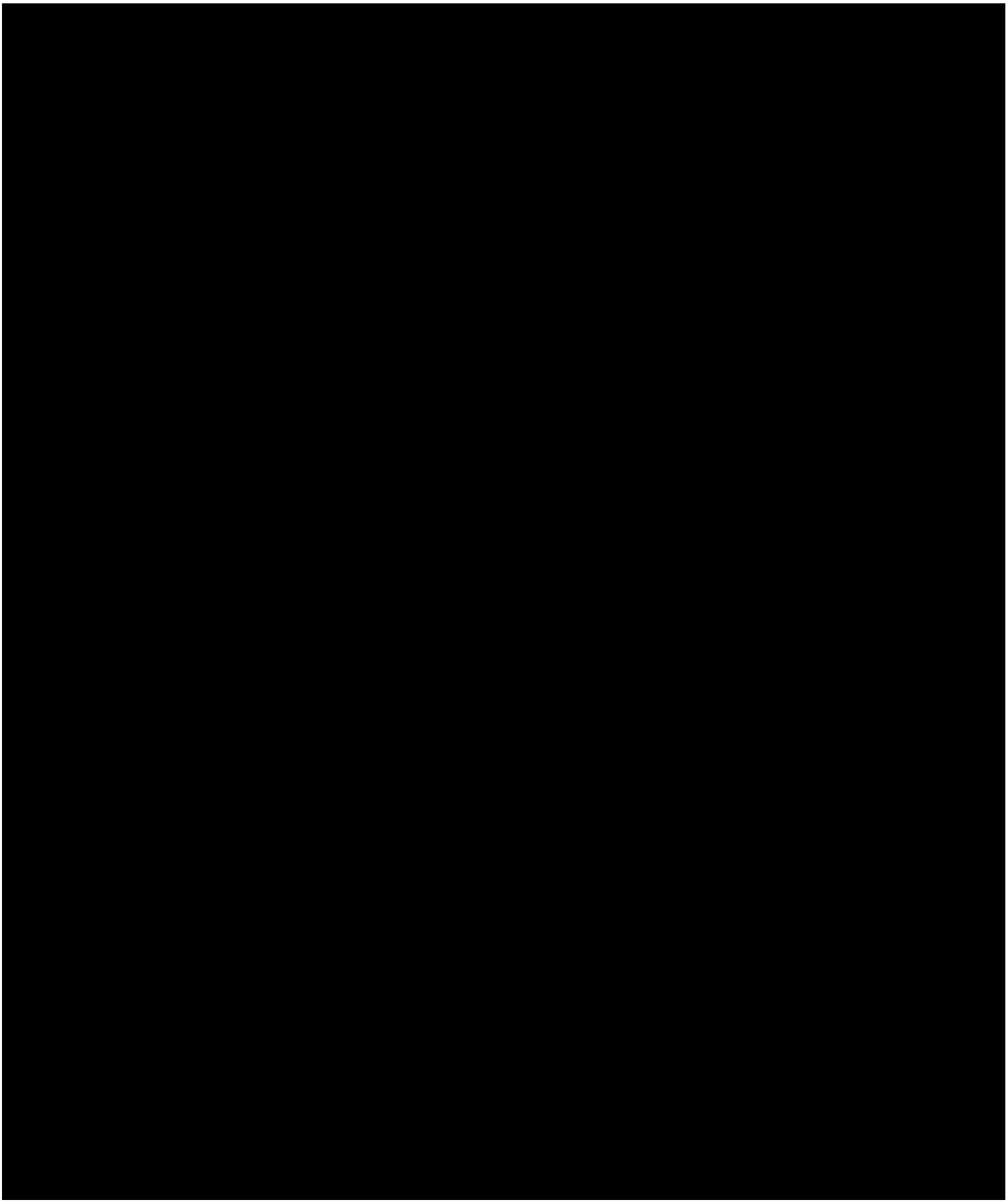








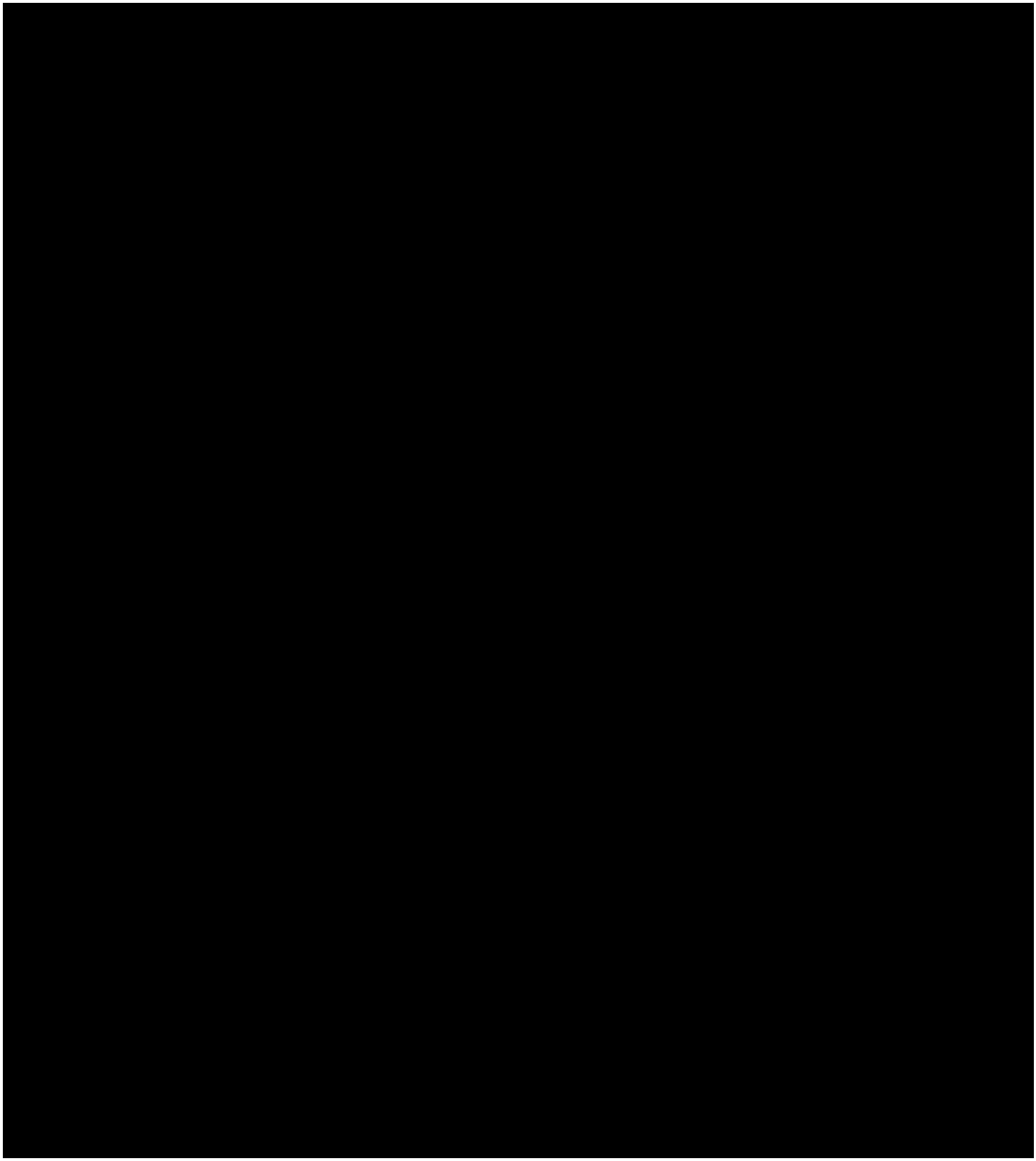


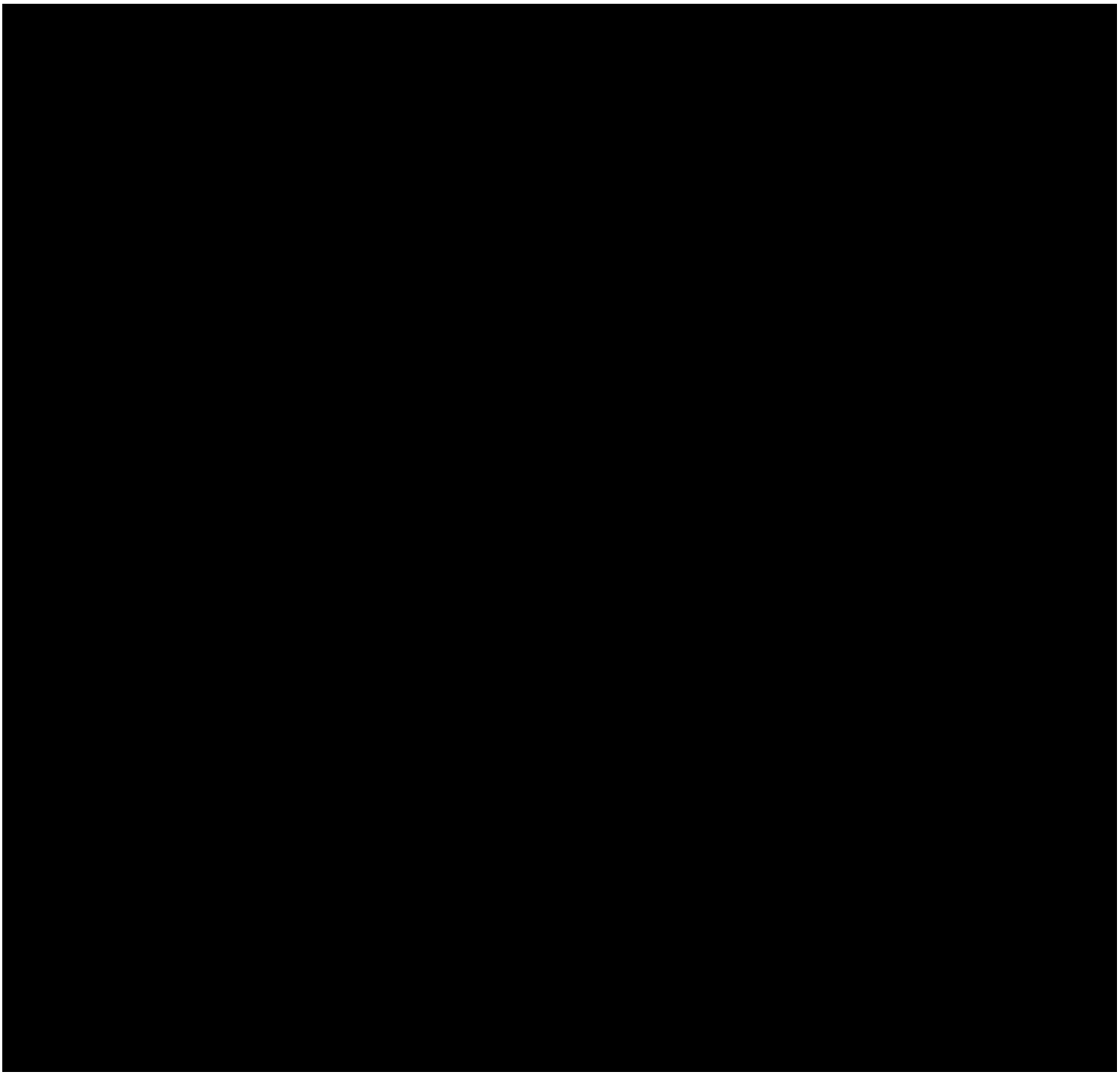


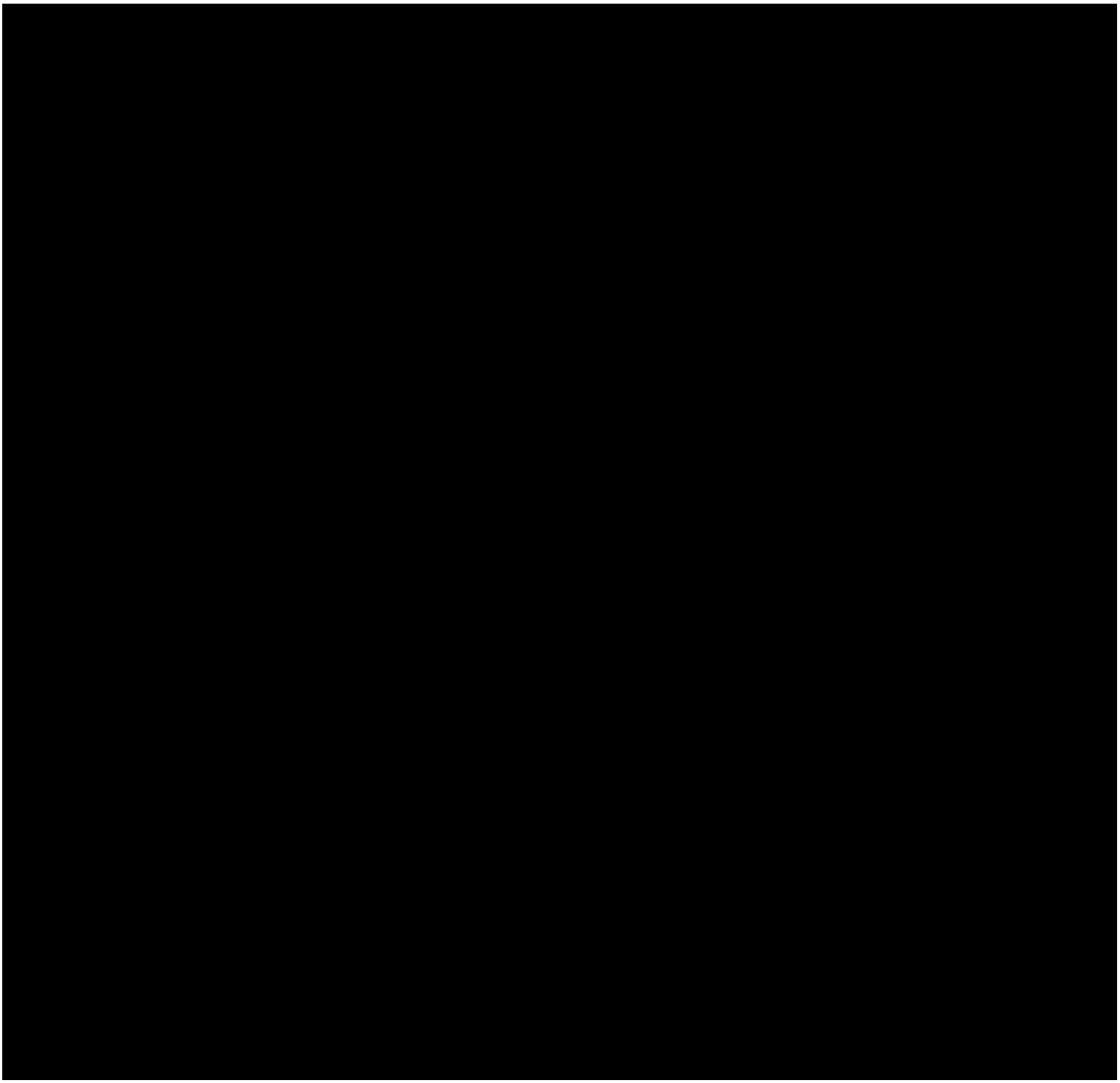
[redacted]

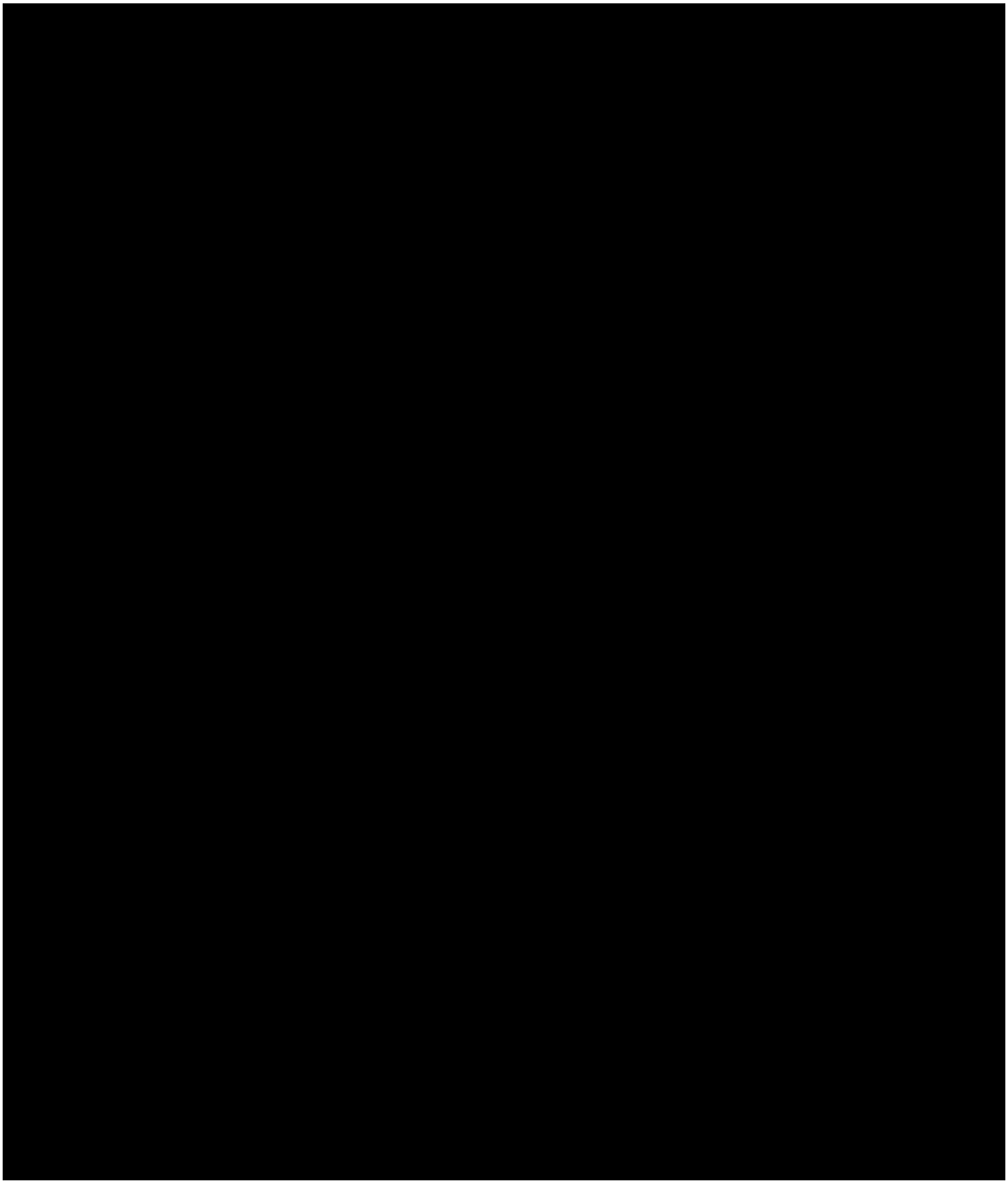
Crown
Commercial

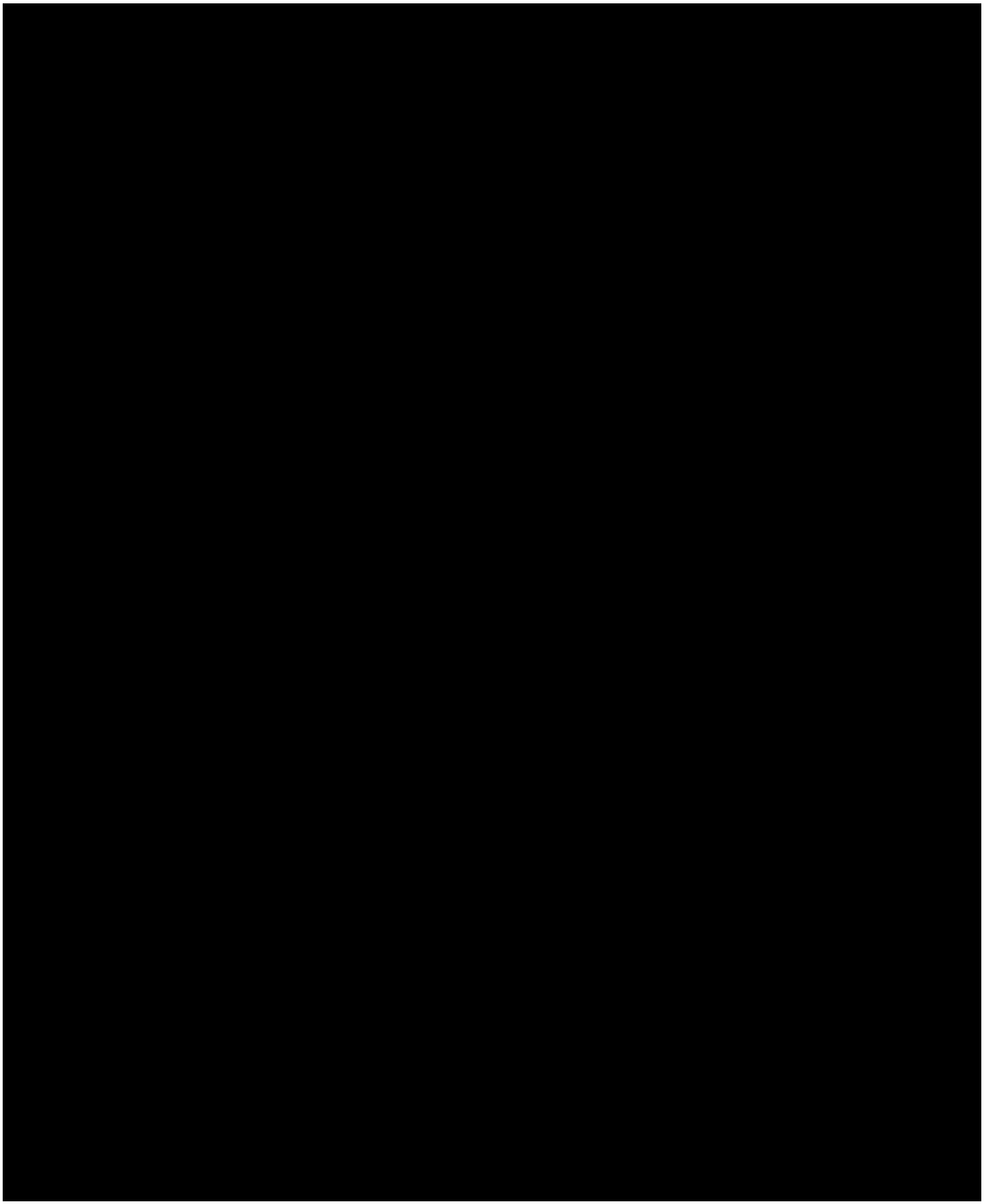
[redacted]



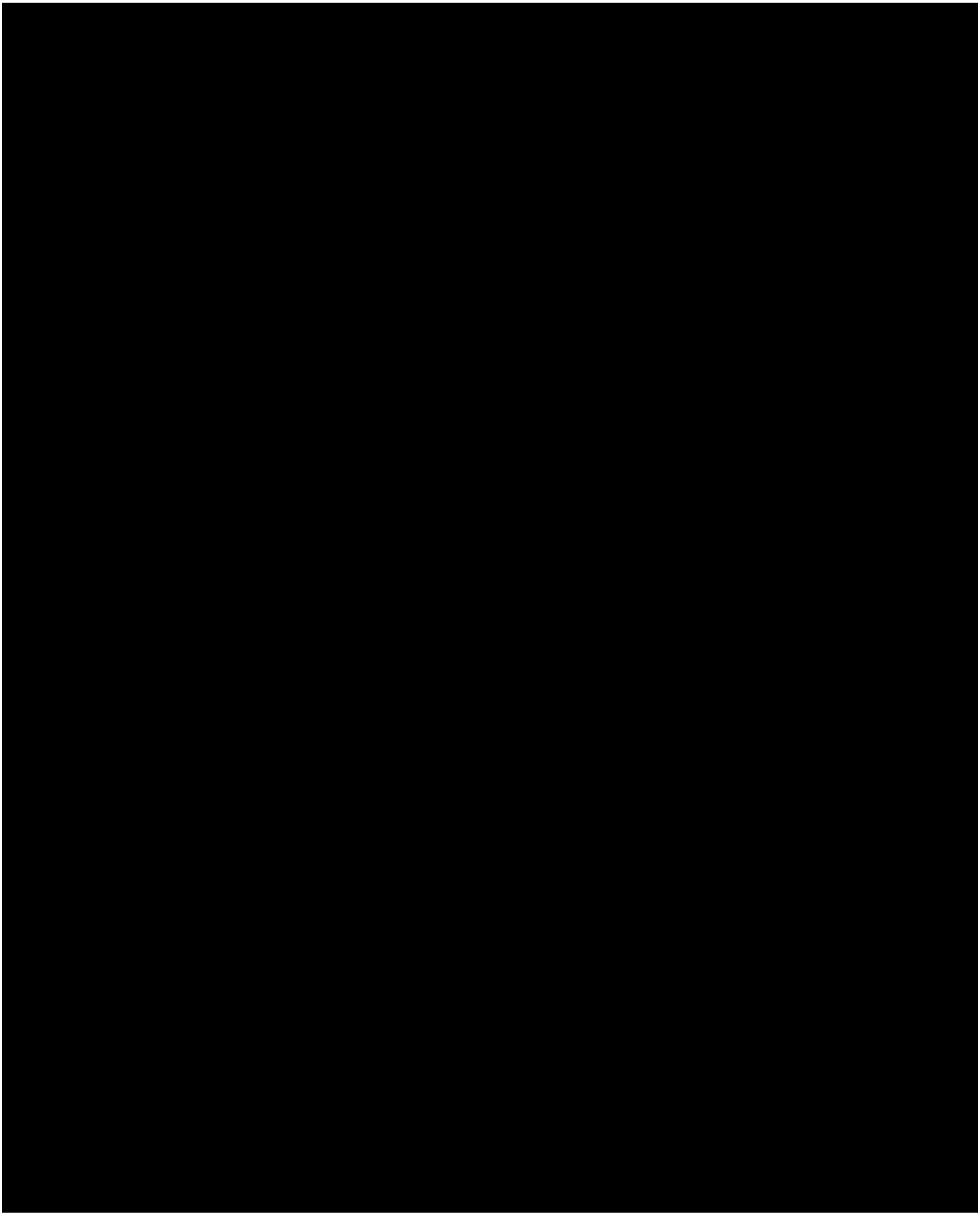


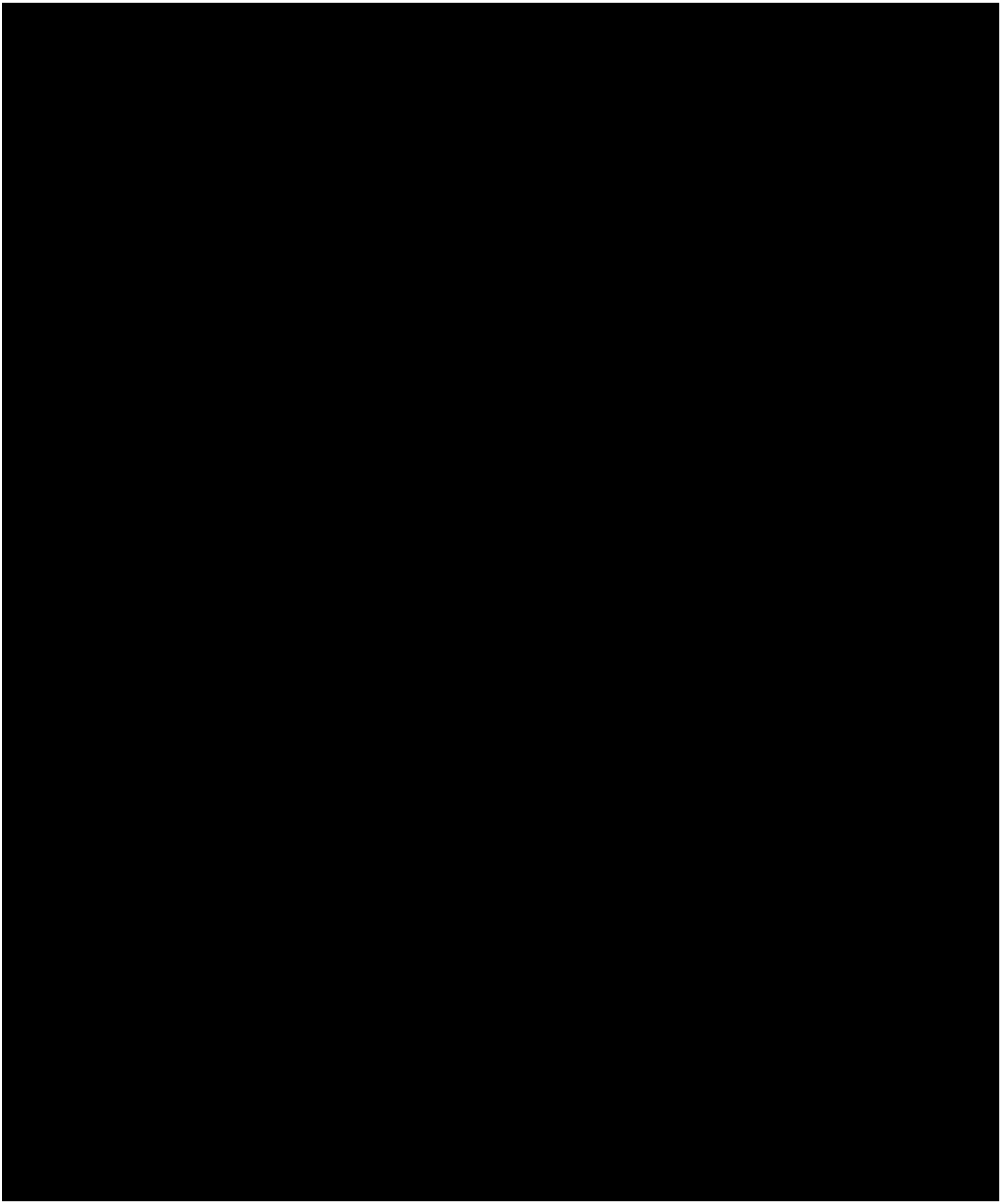


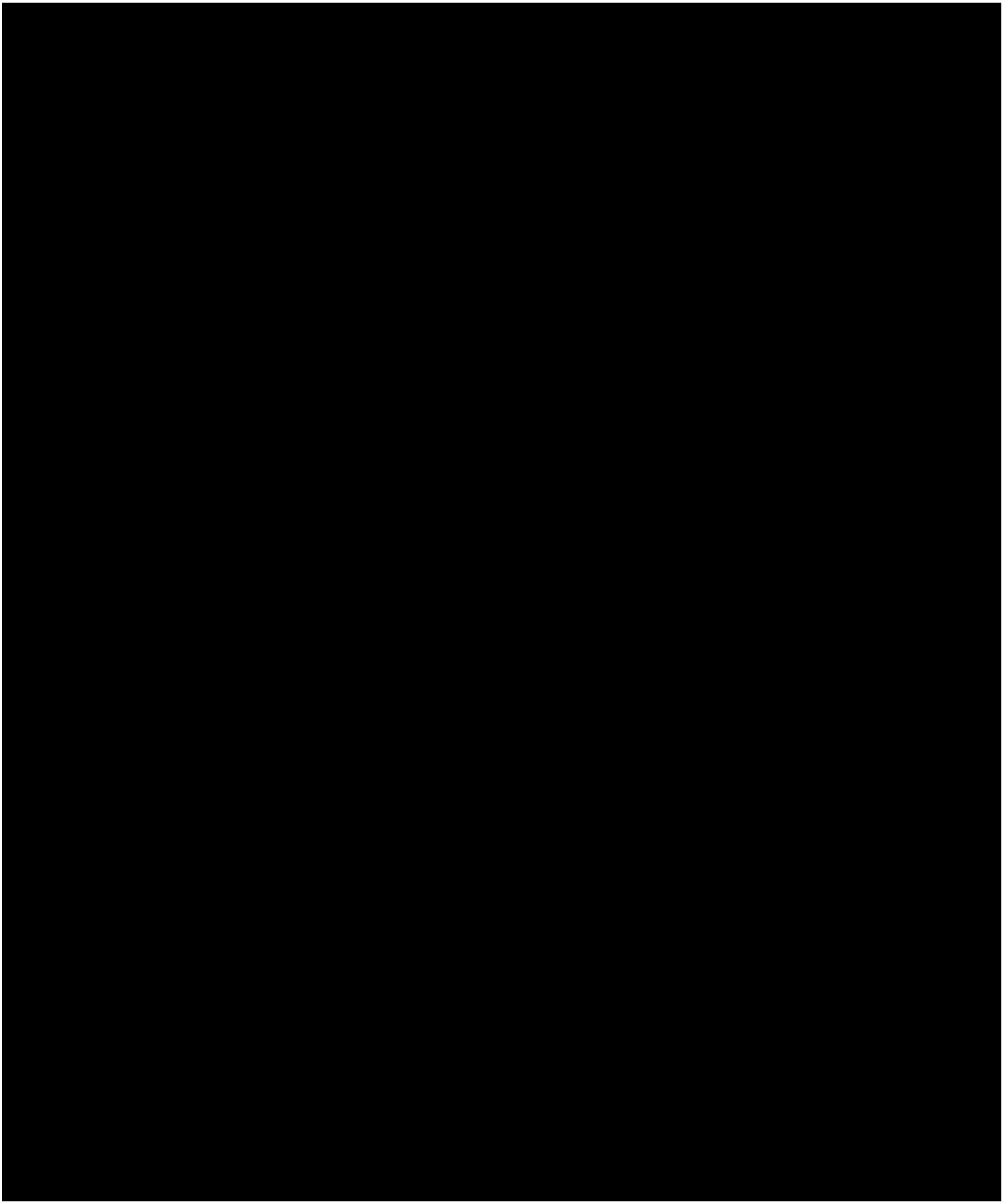




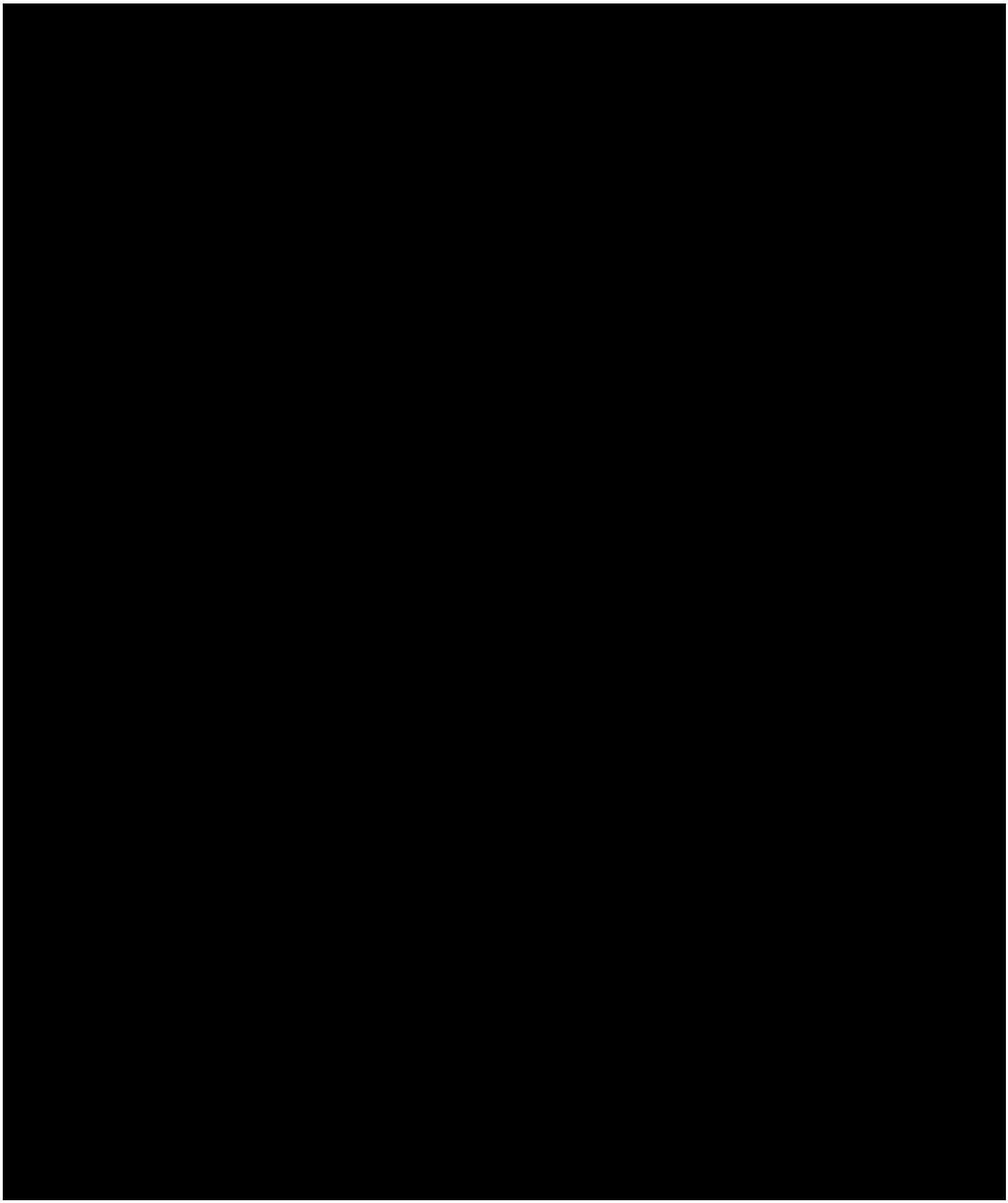
Crown
Commercial

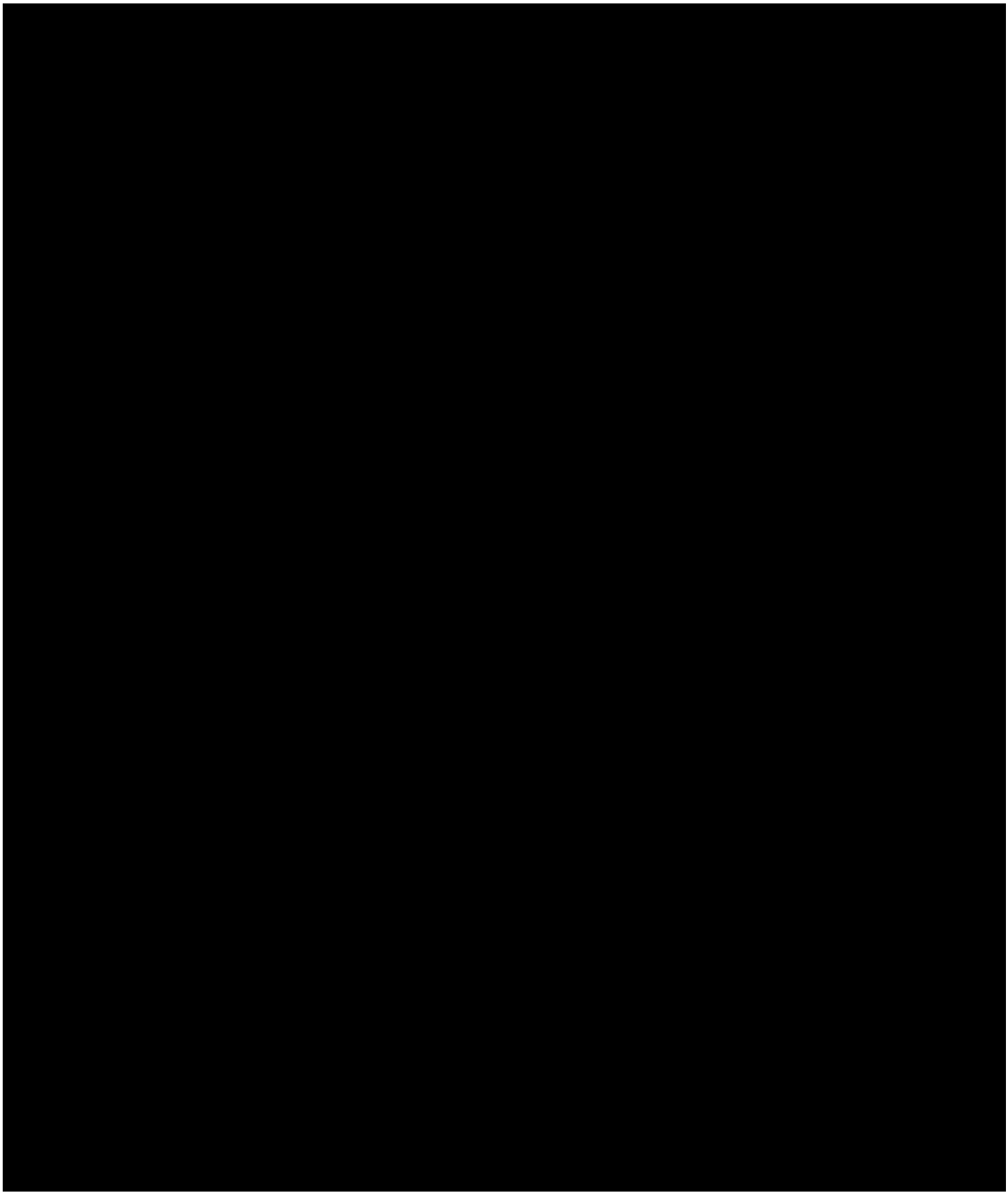


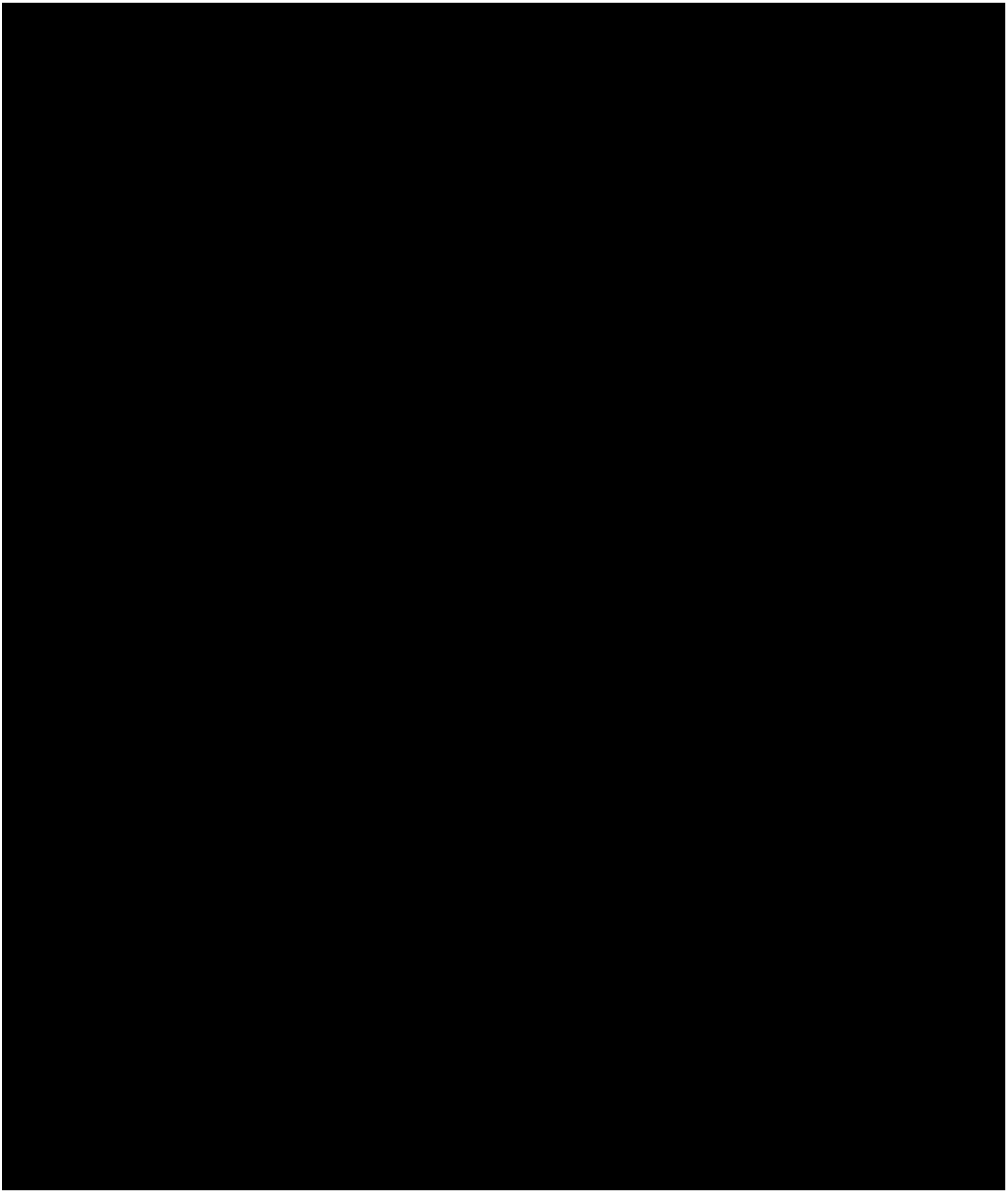


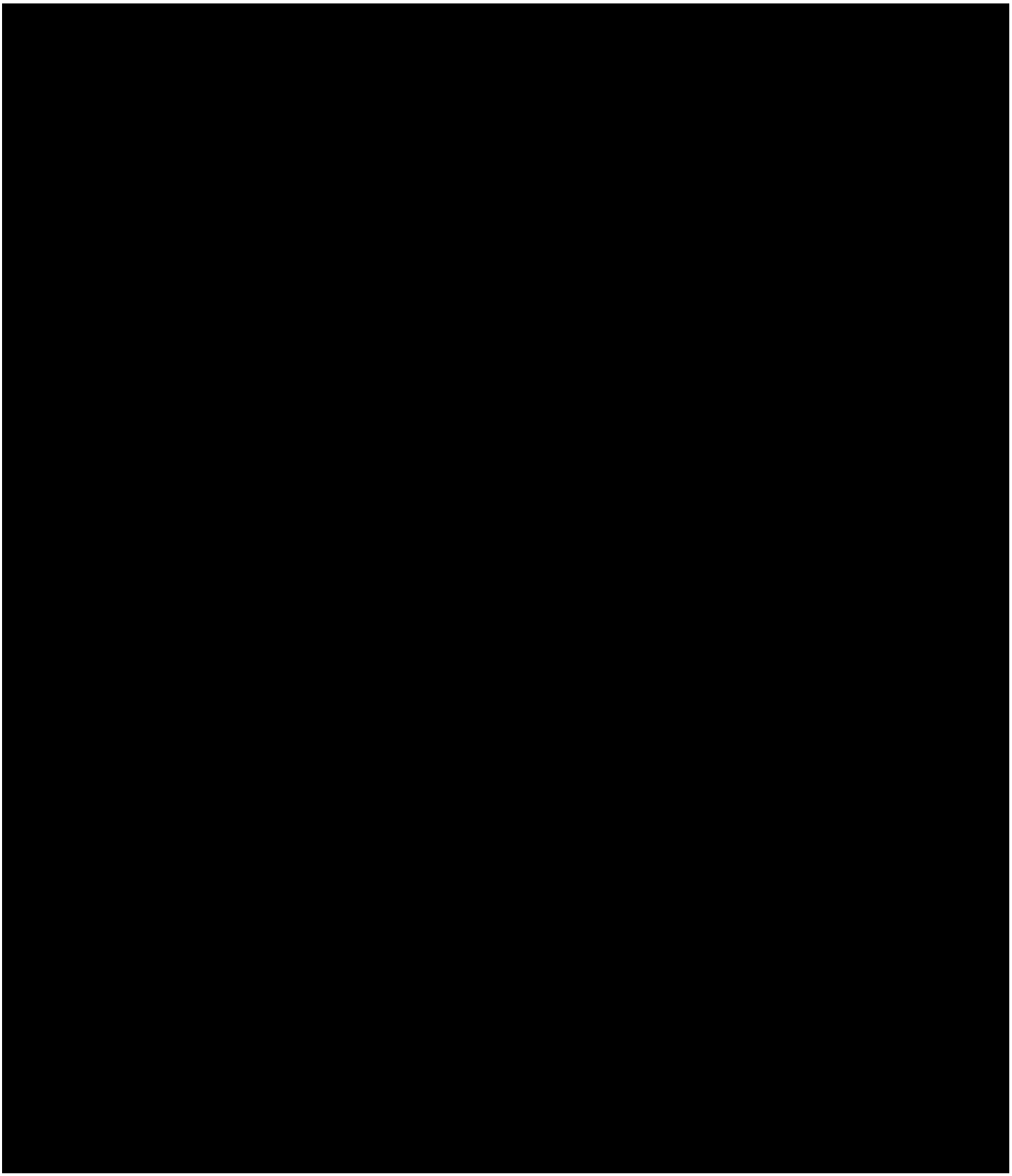


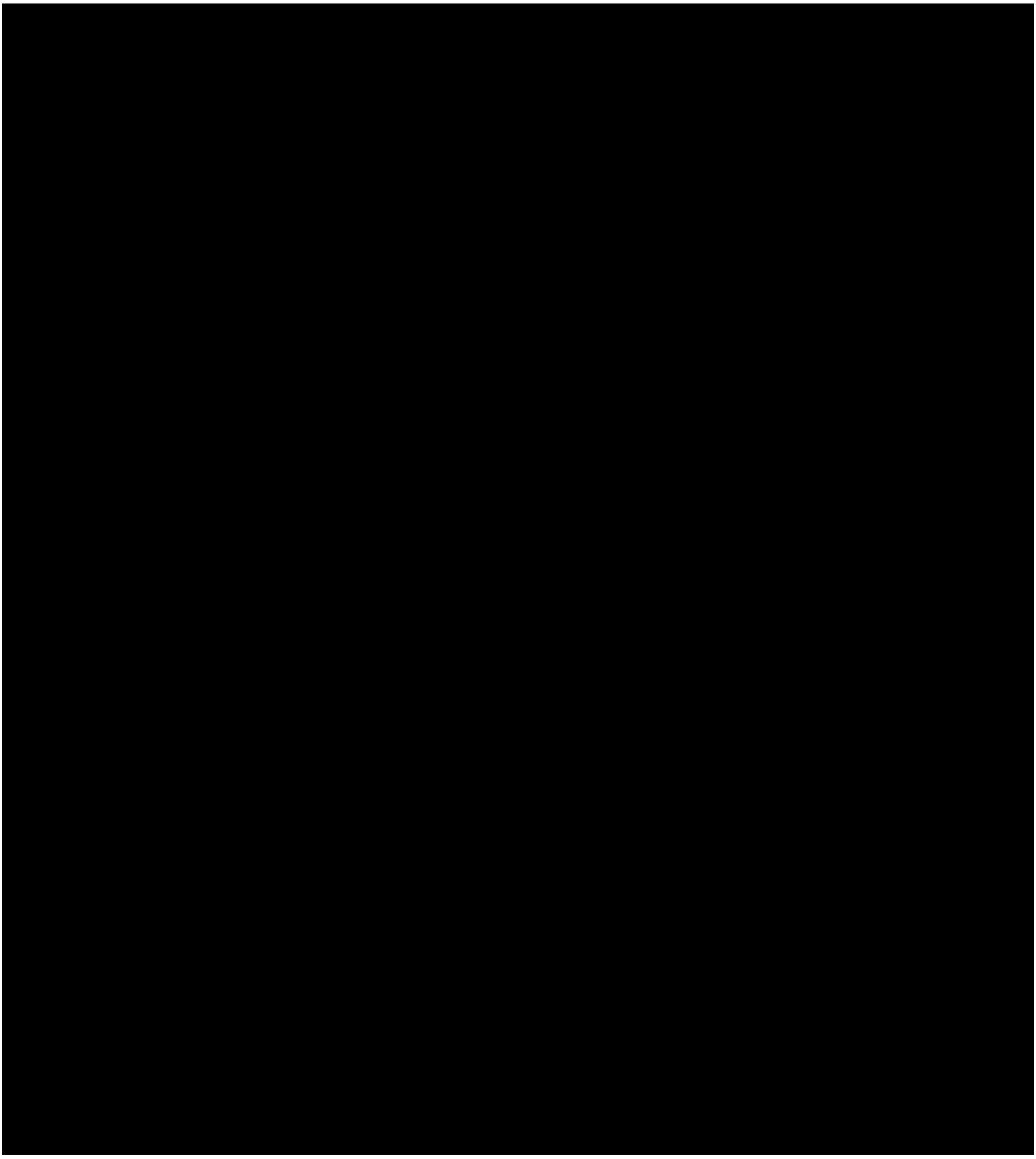
Crown Commercial

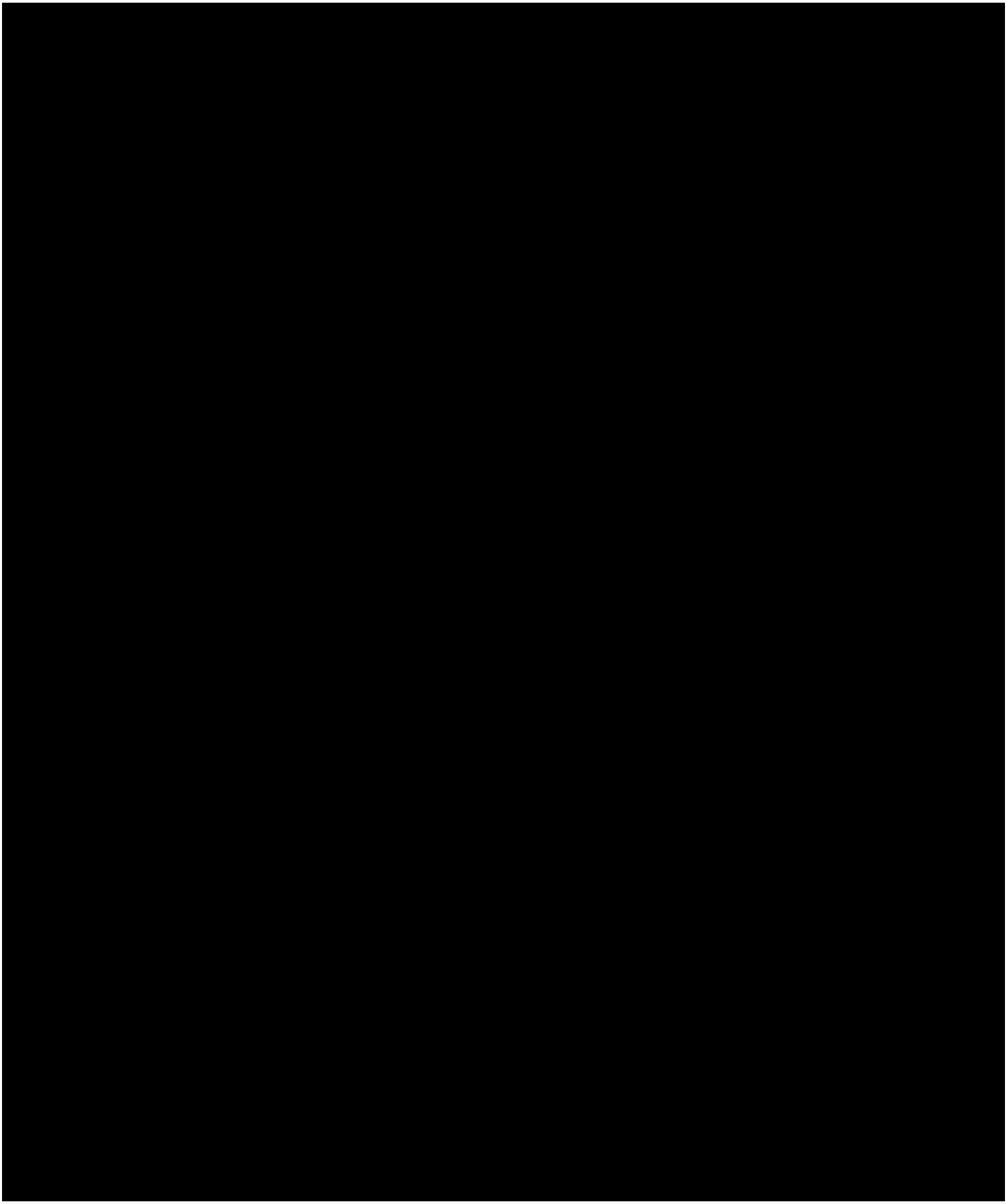


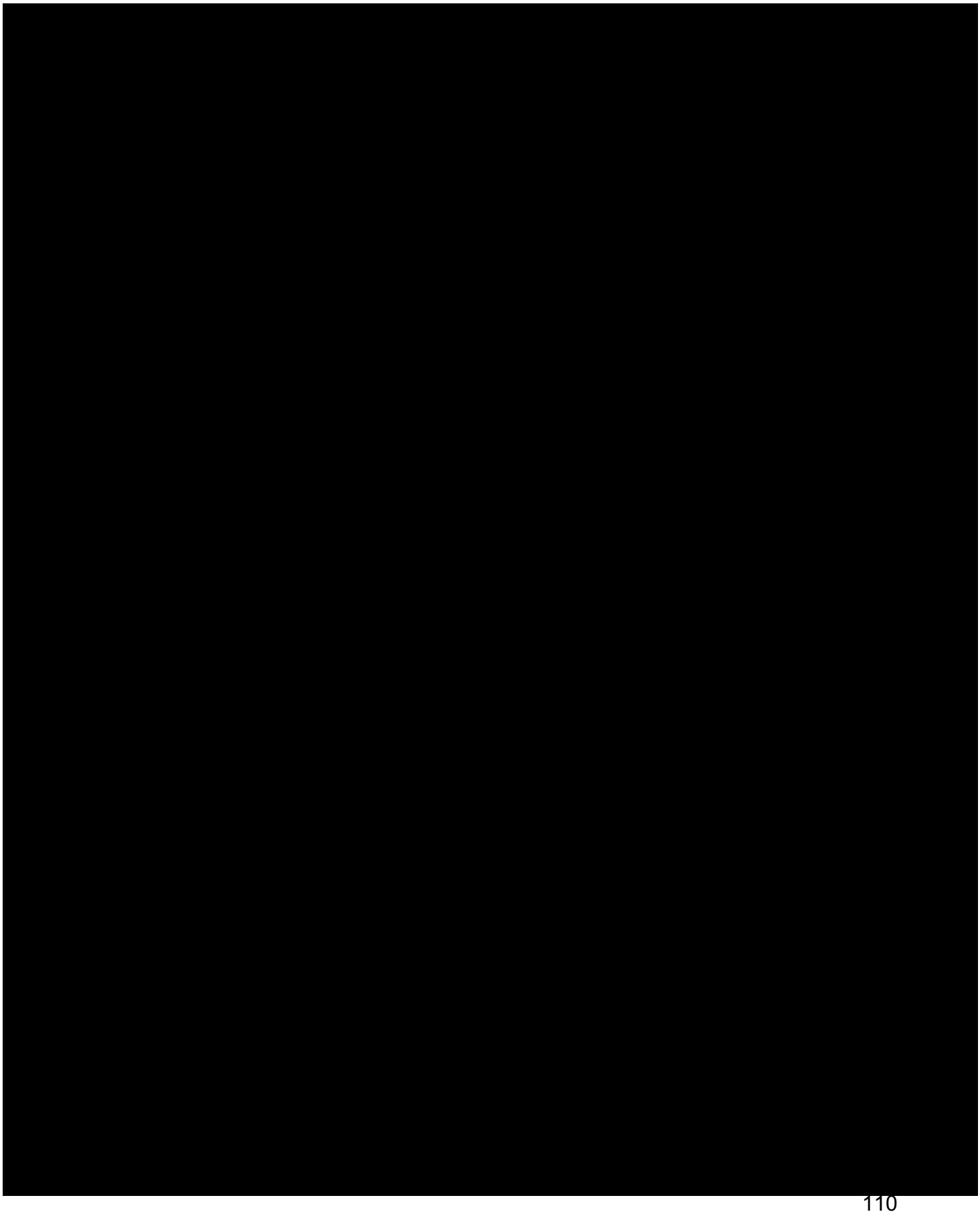


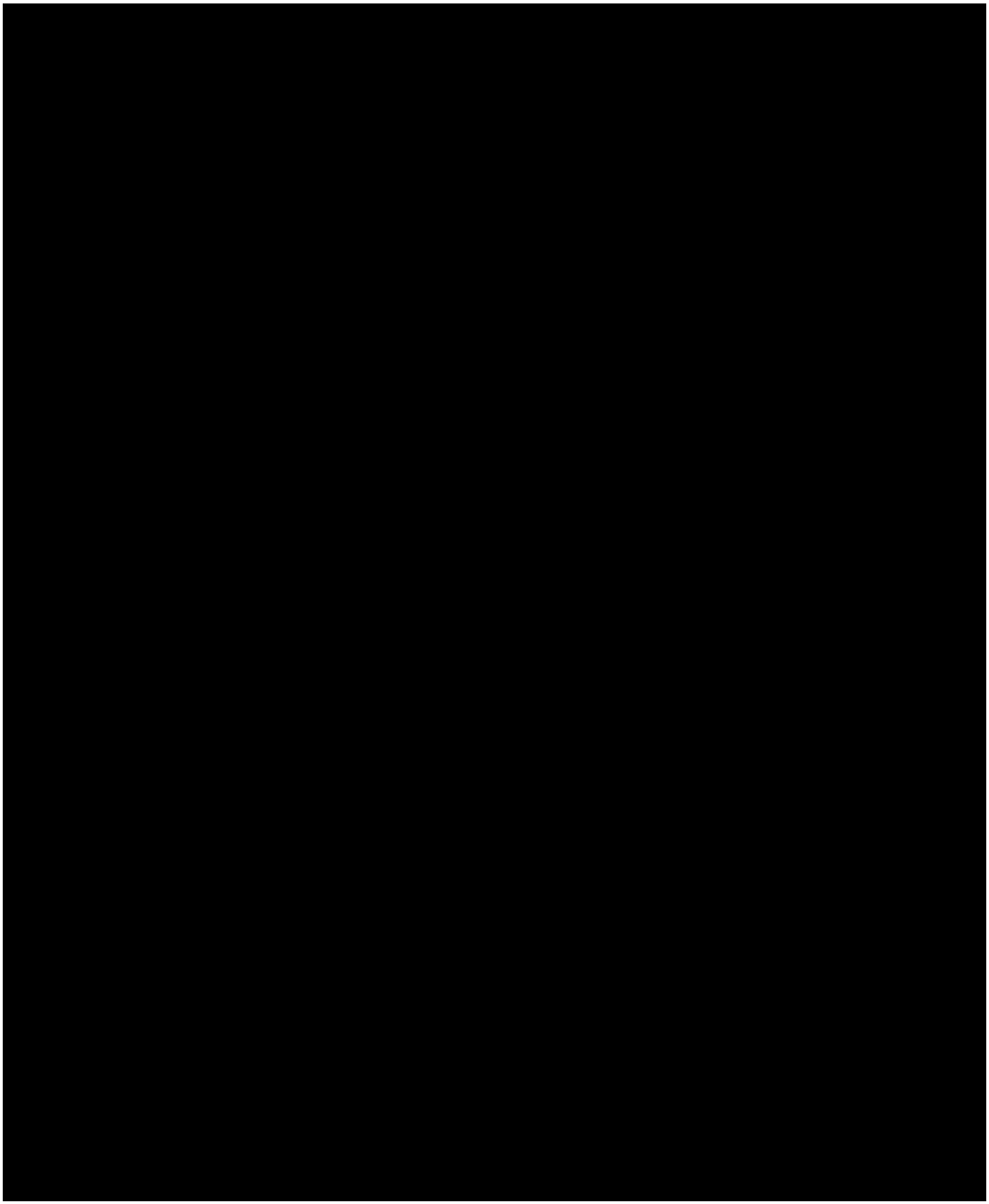




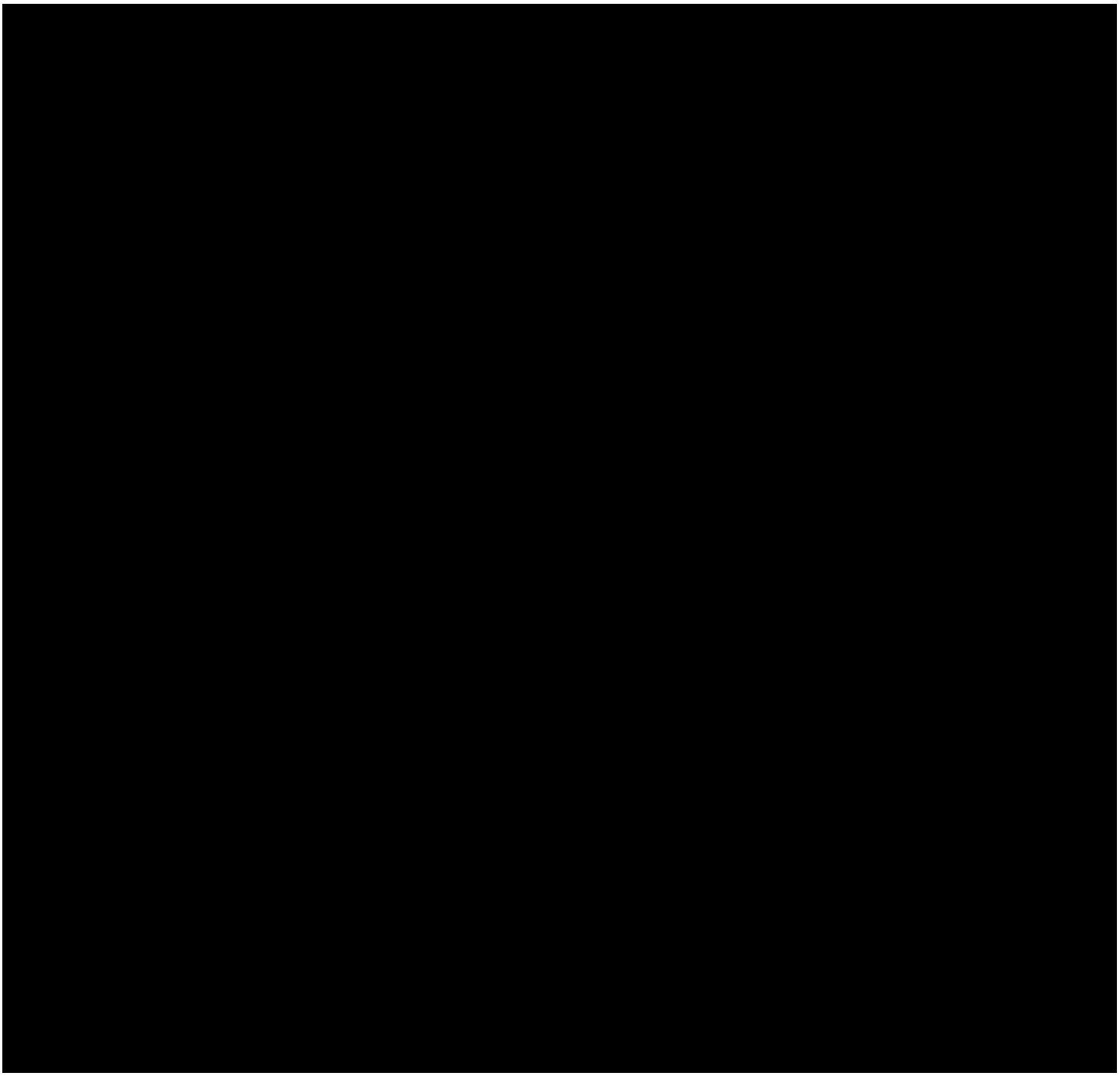


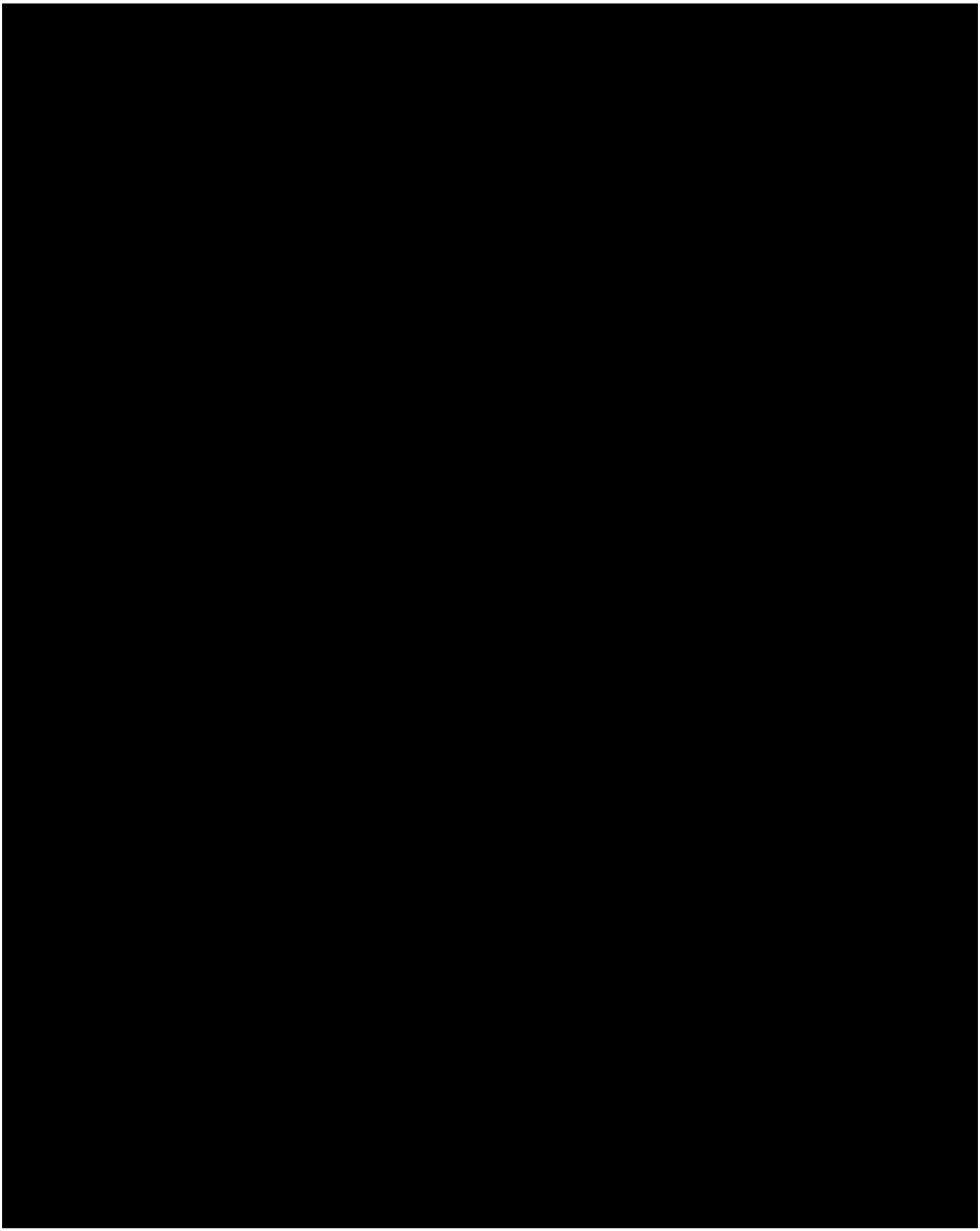


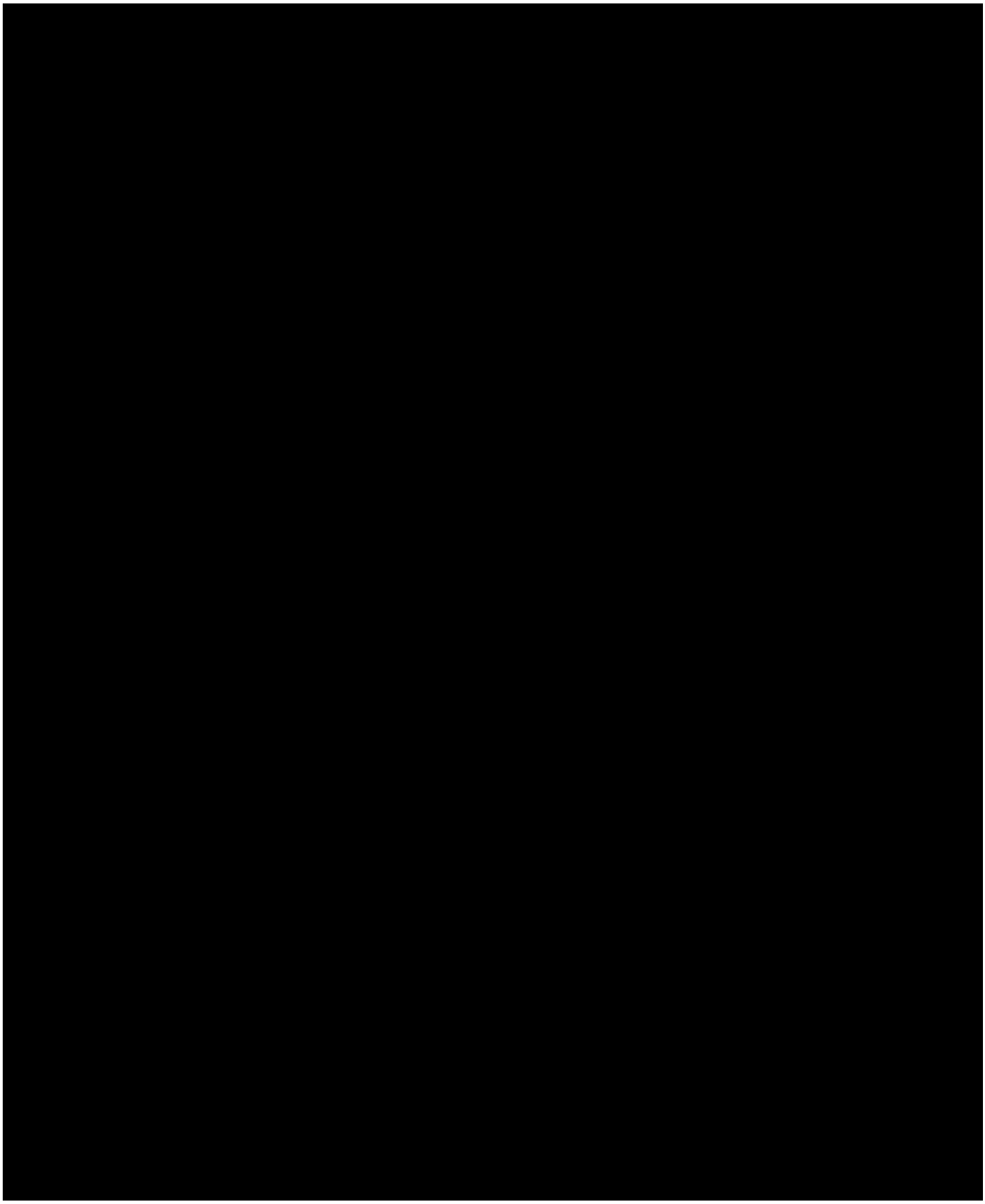




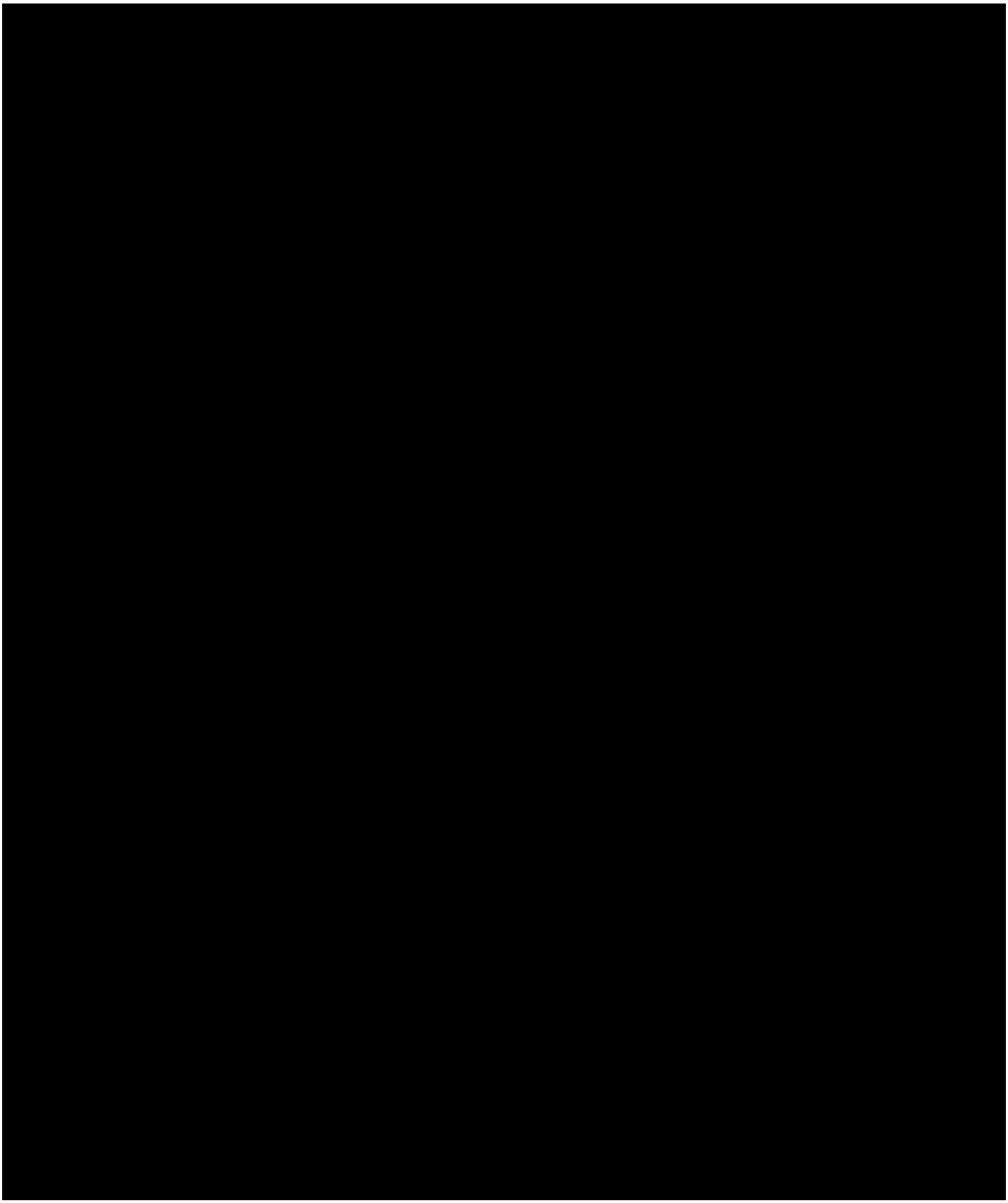
Crown
Commercial



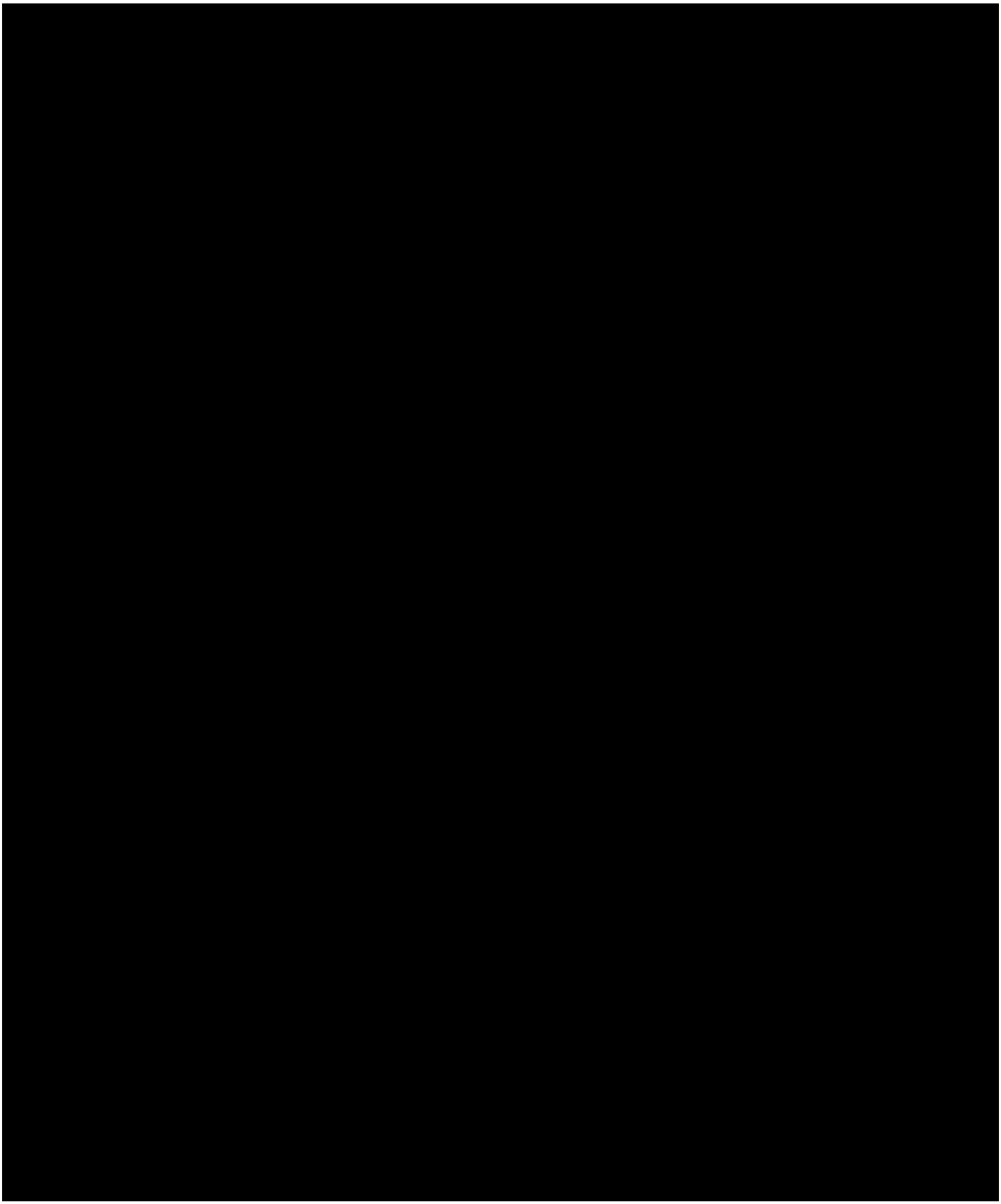


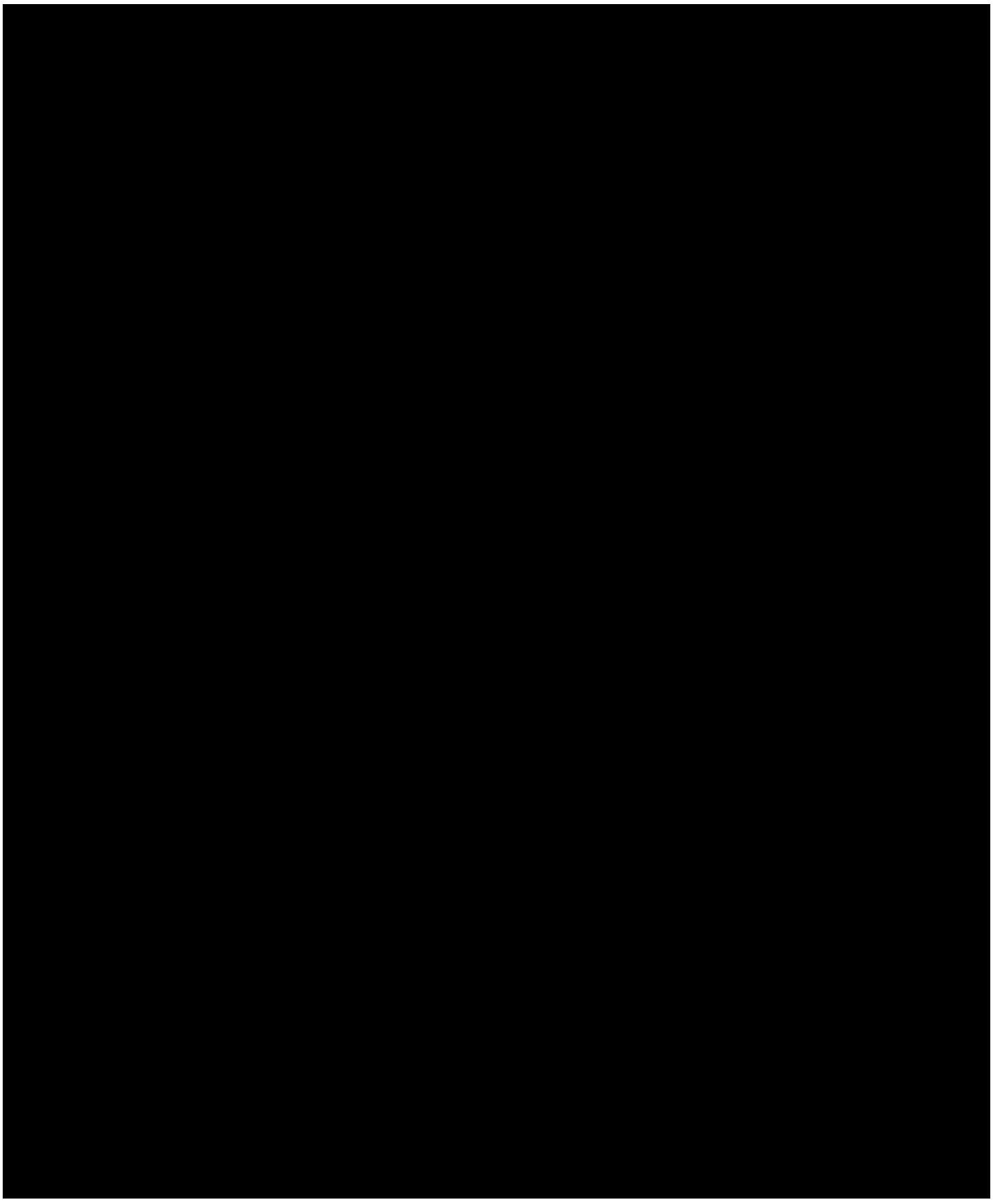


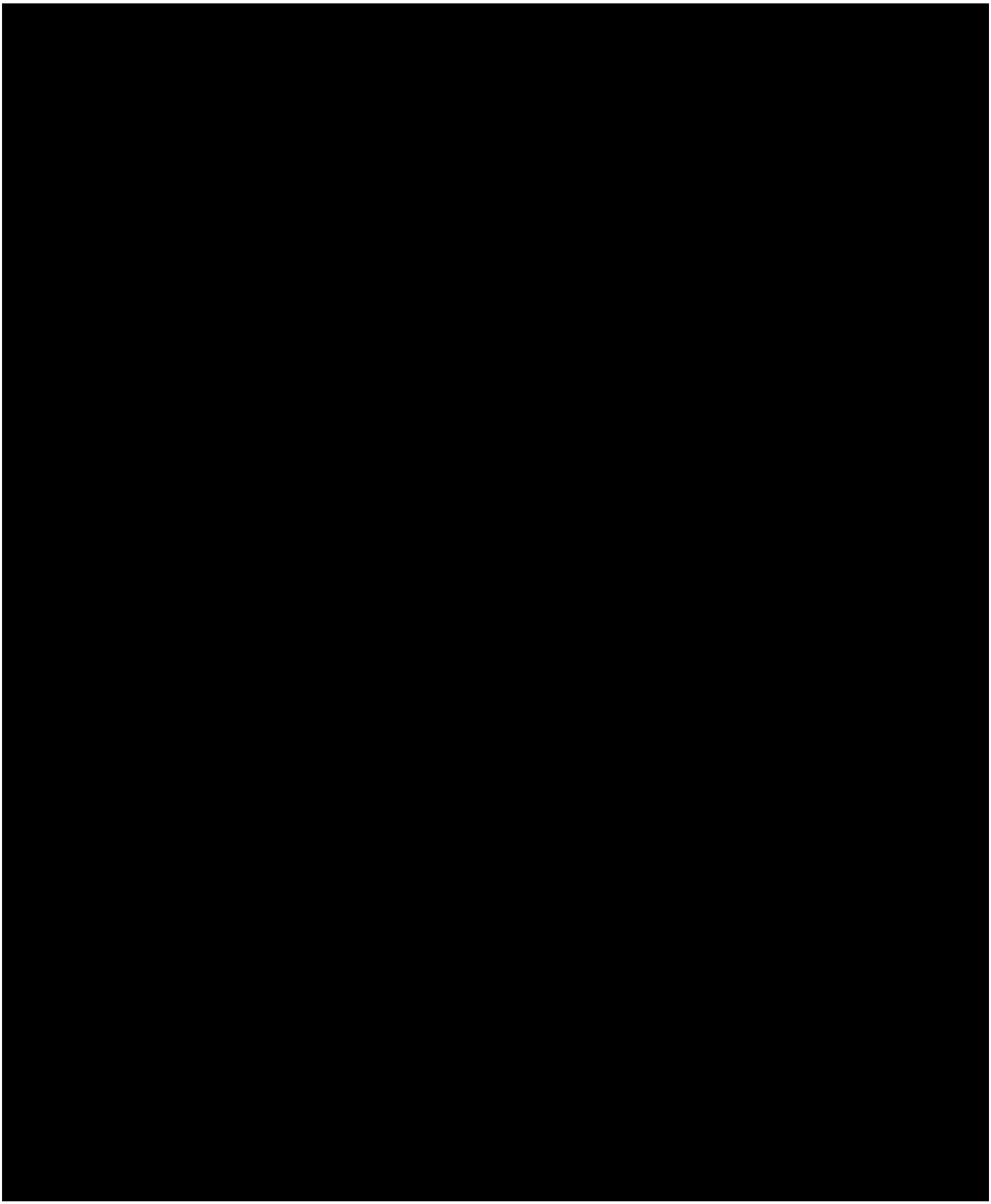
Crown Commercial

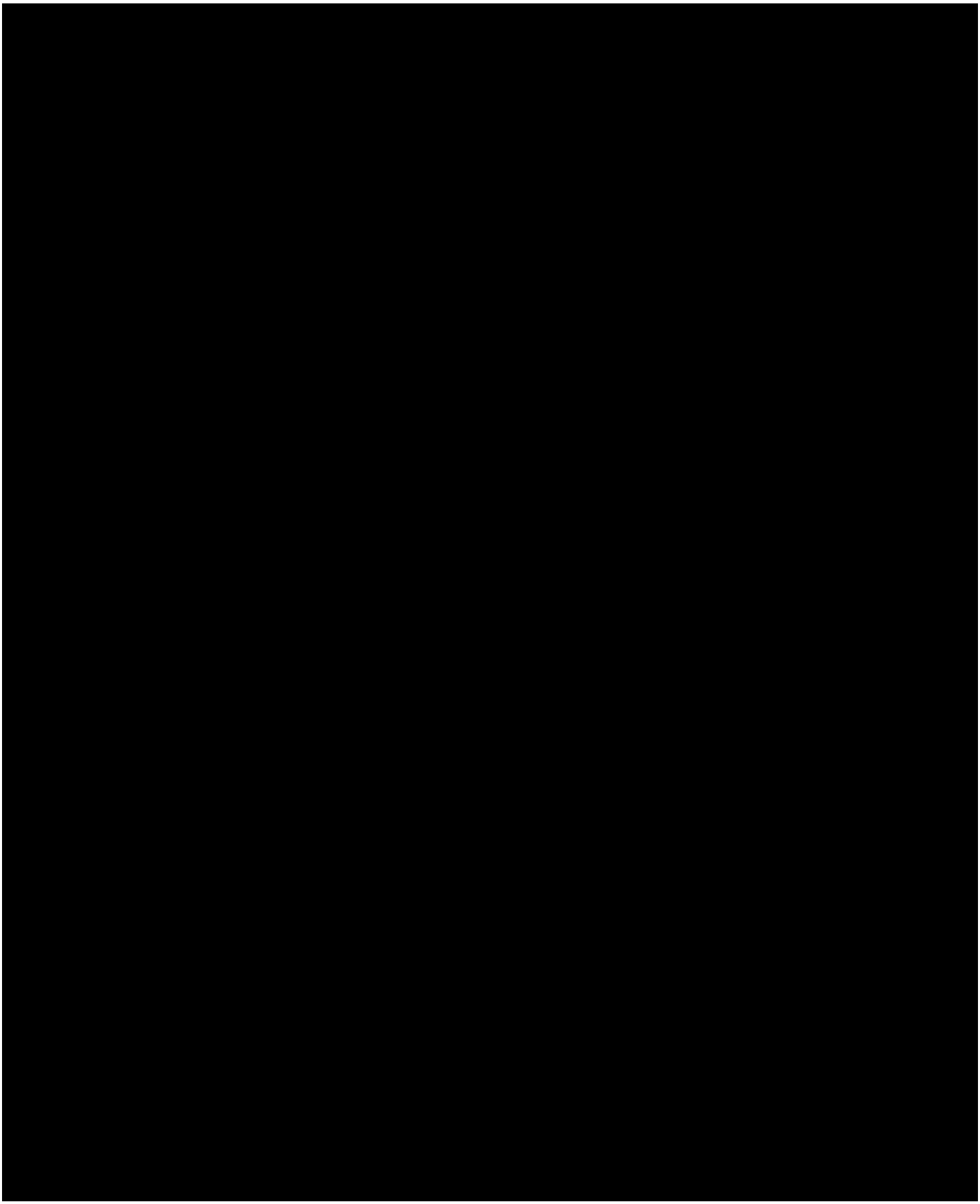


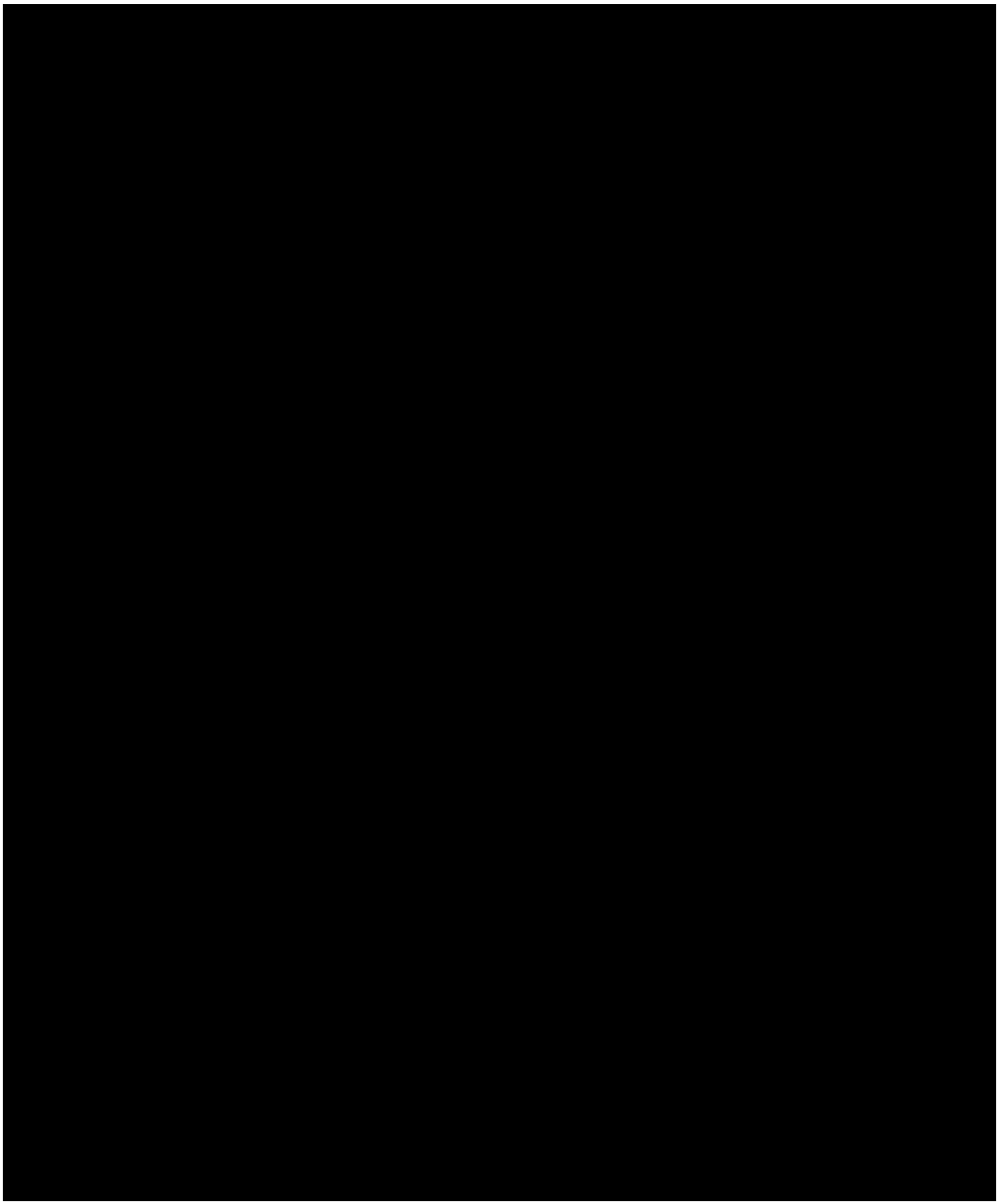
Crown Commercial



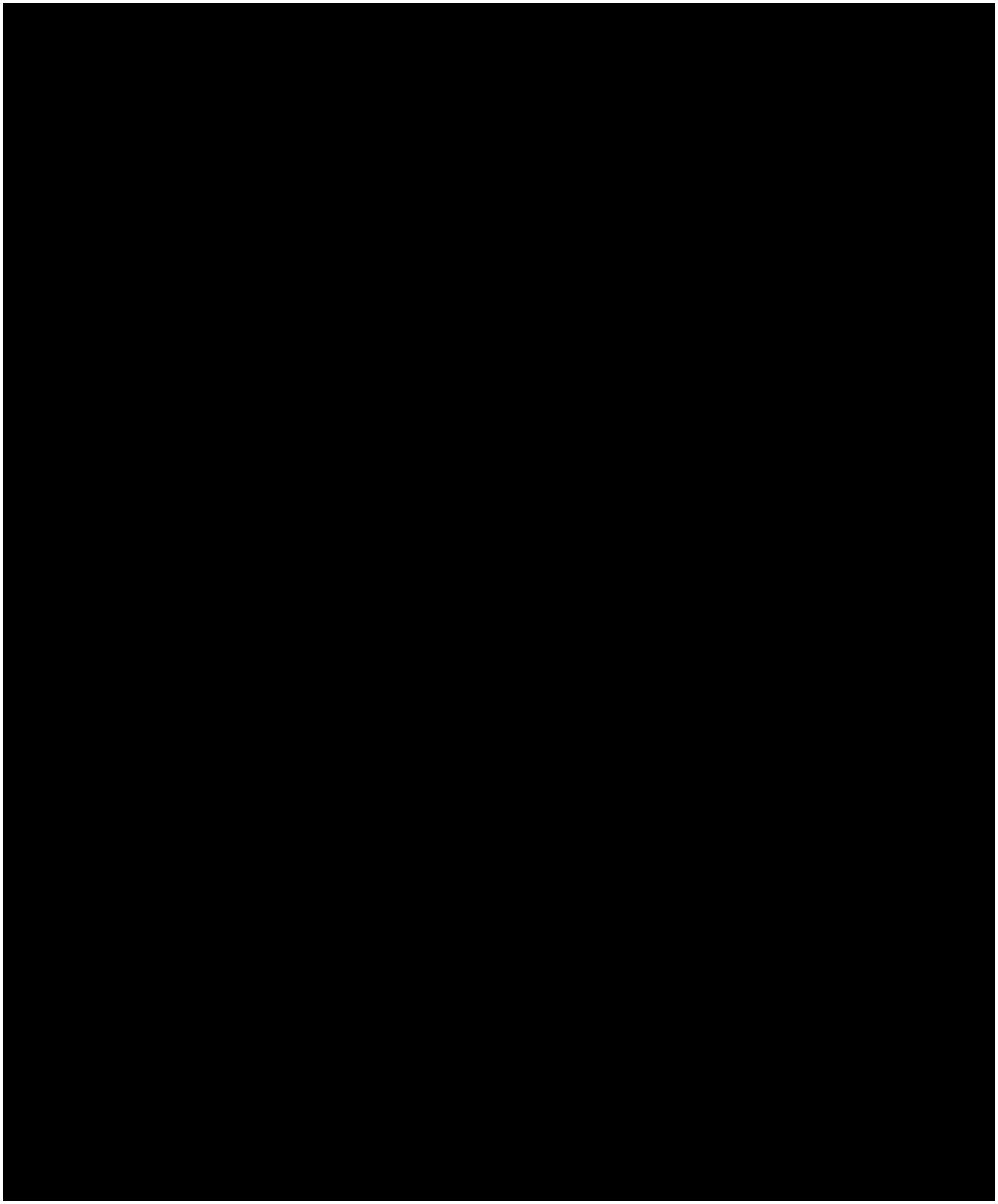


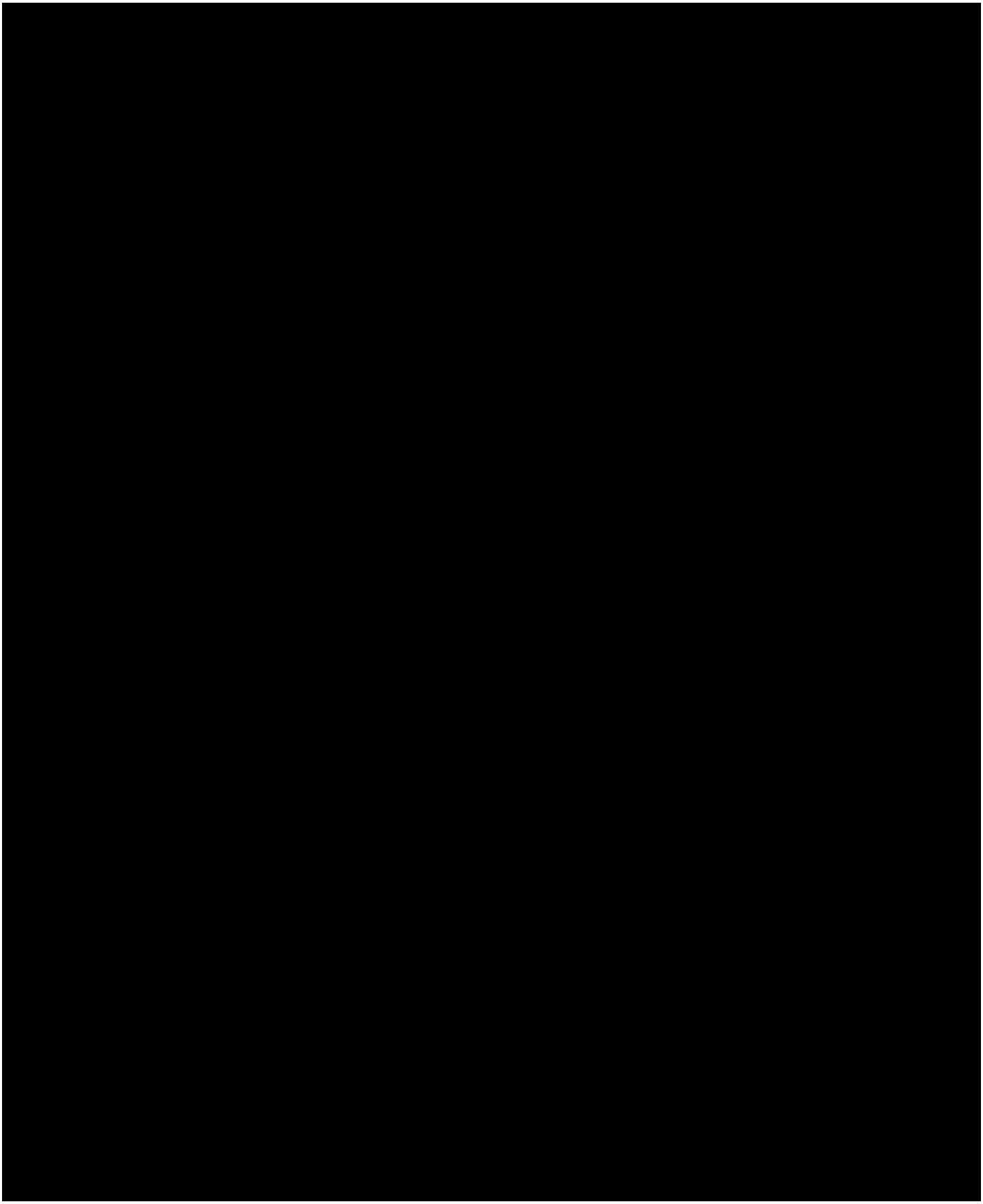




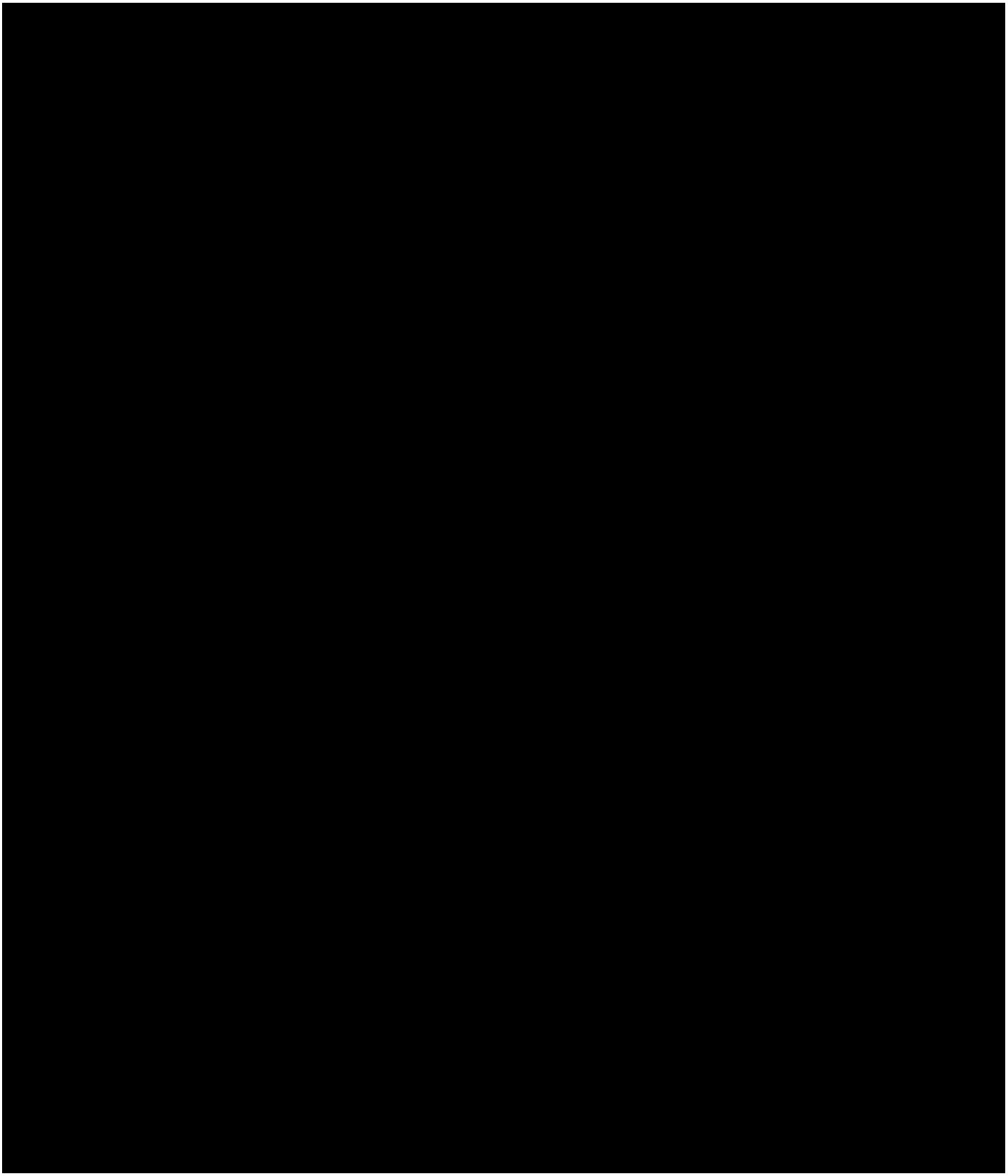


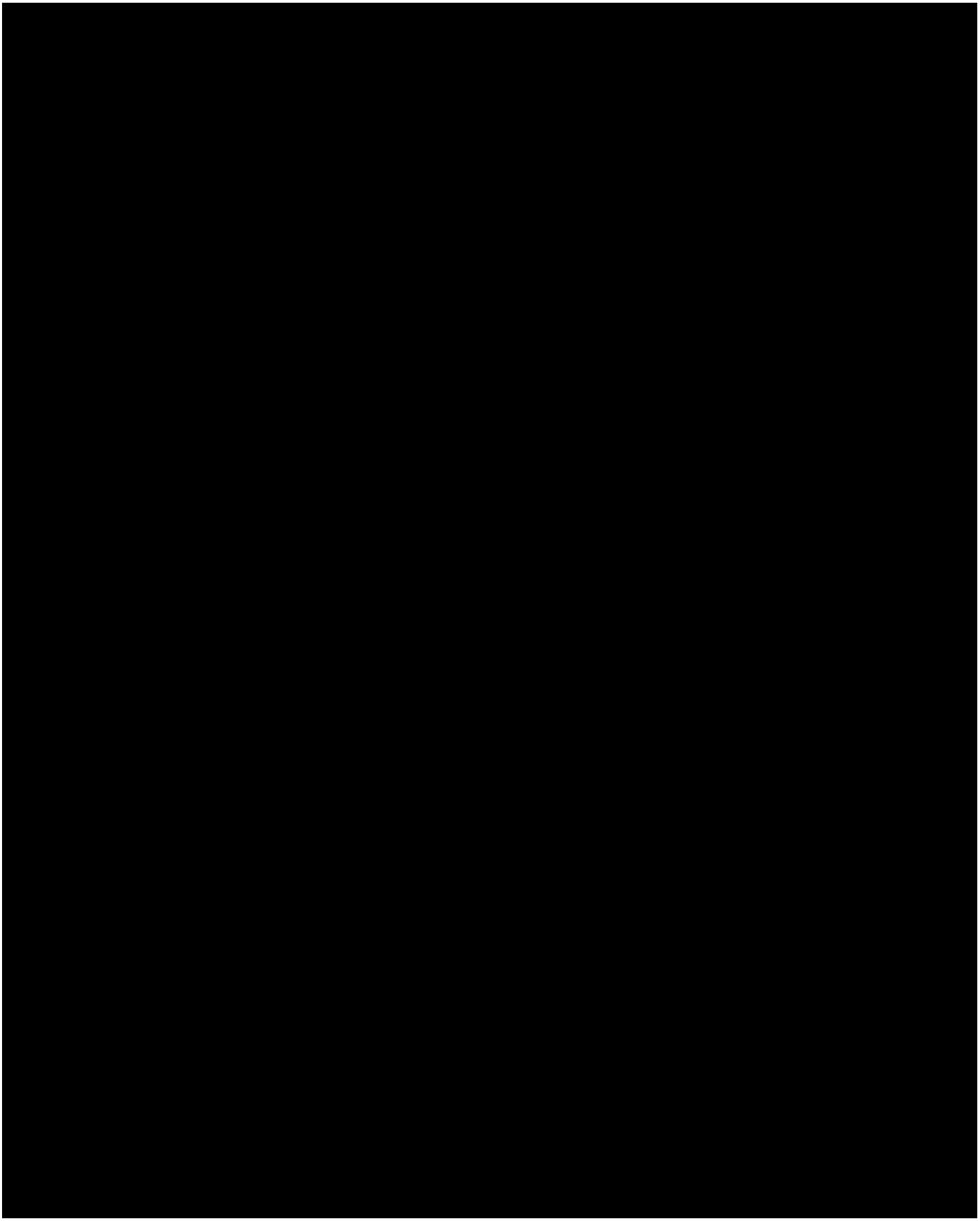
Crown Commercial

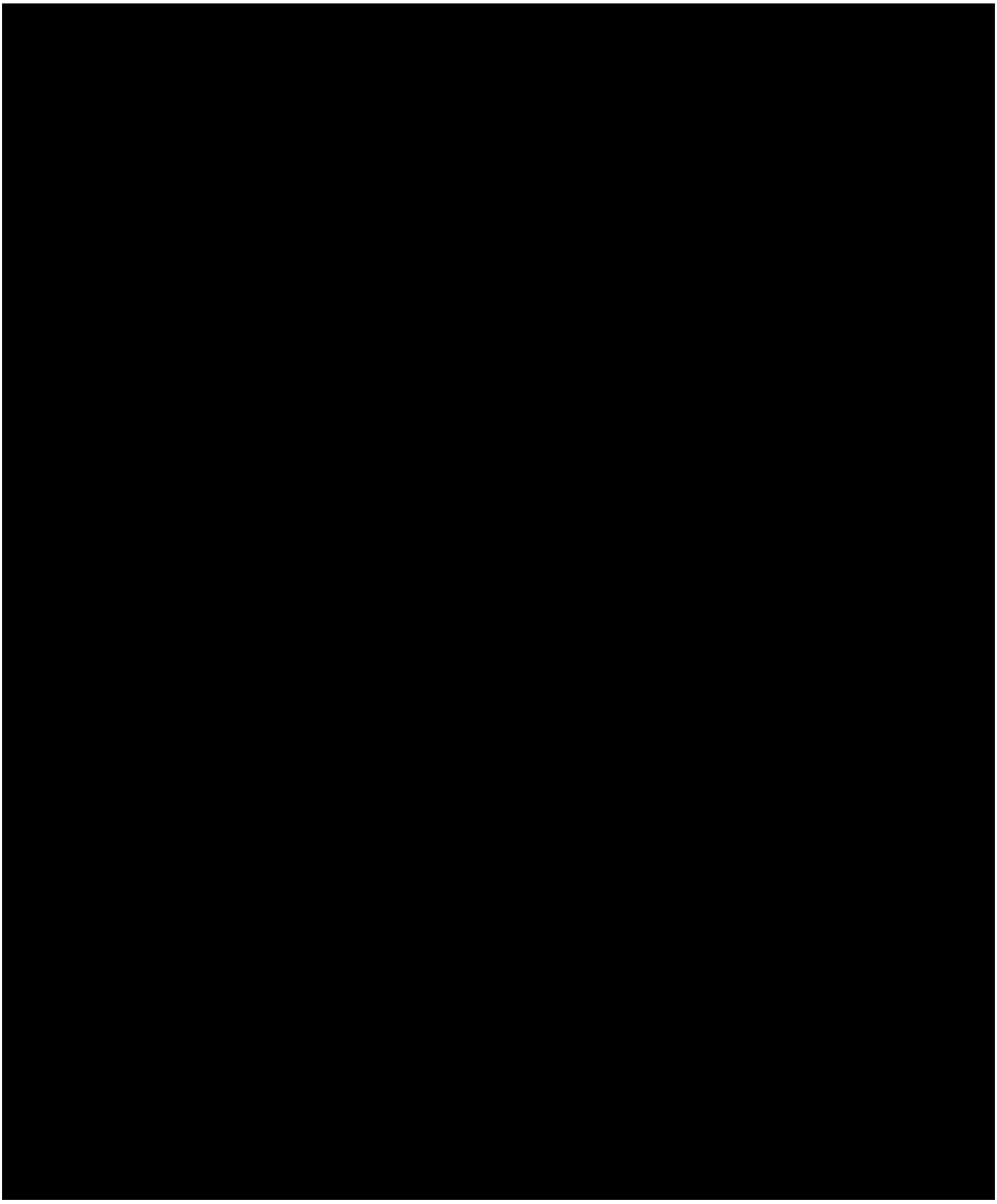


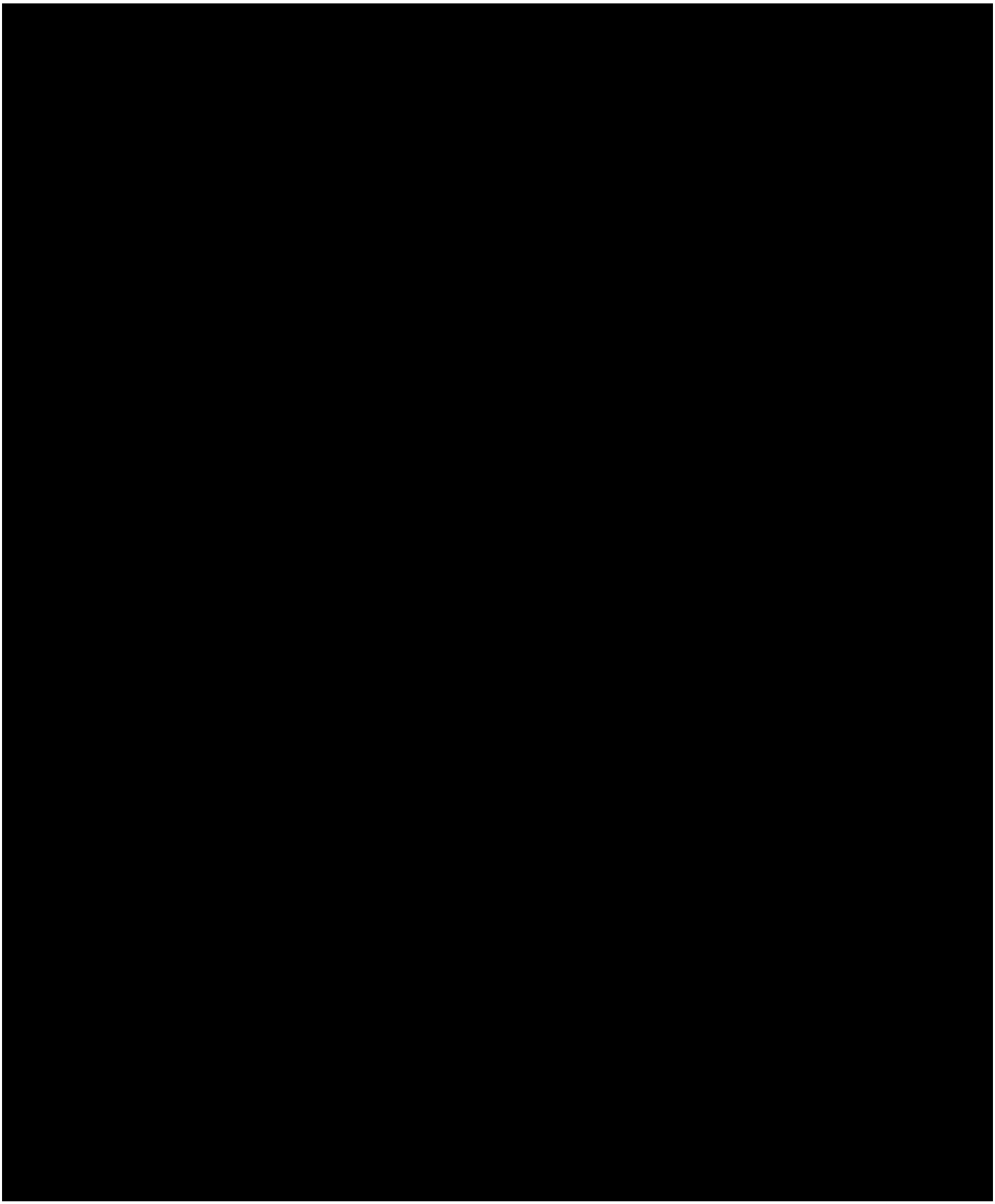


[redacted]

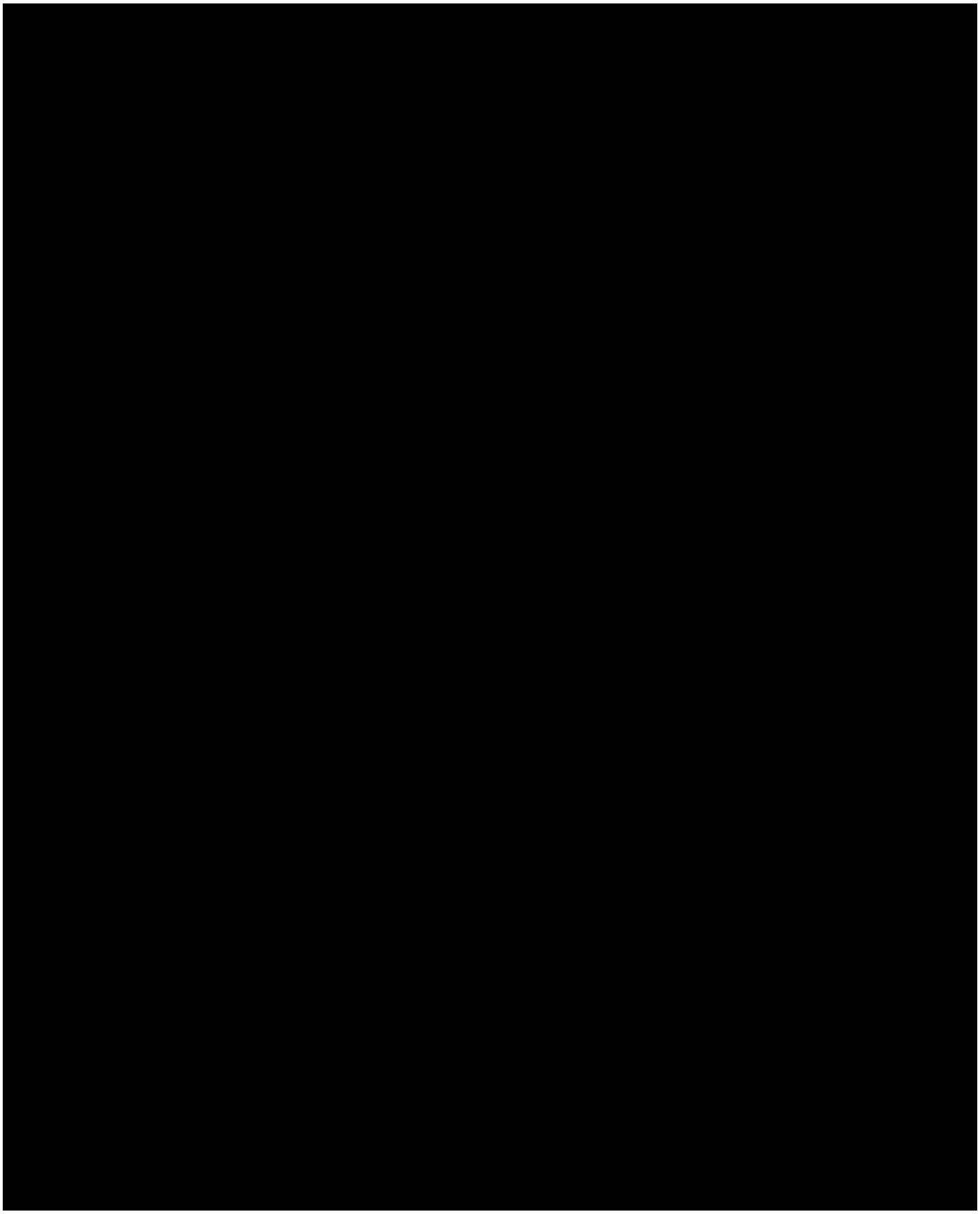


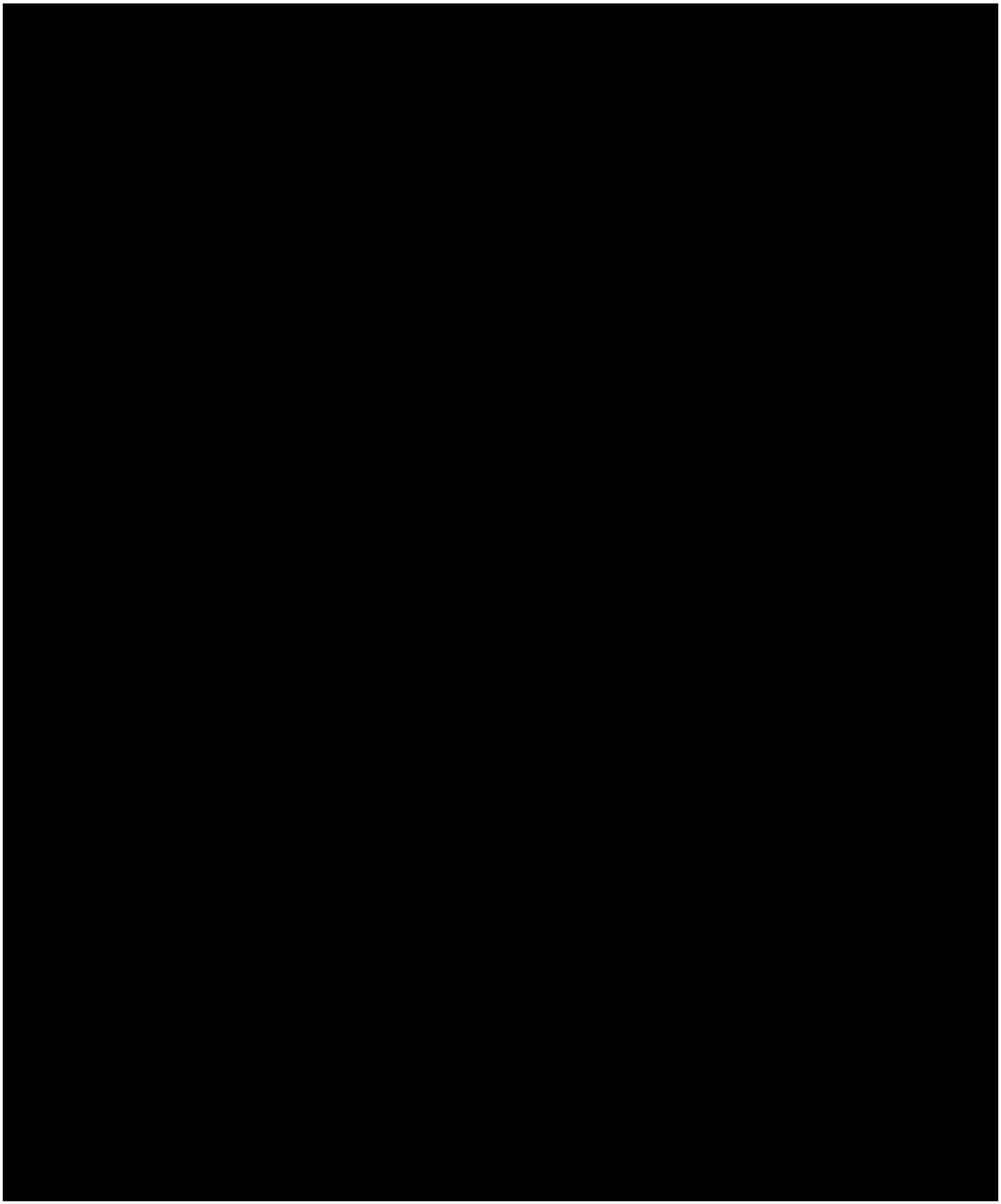


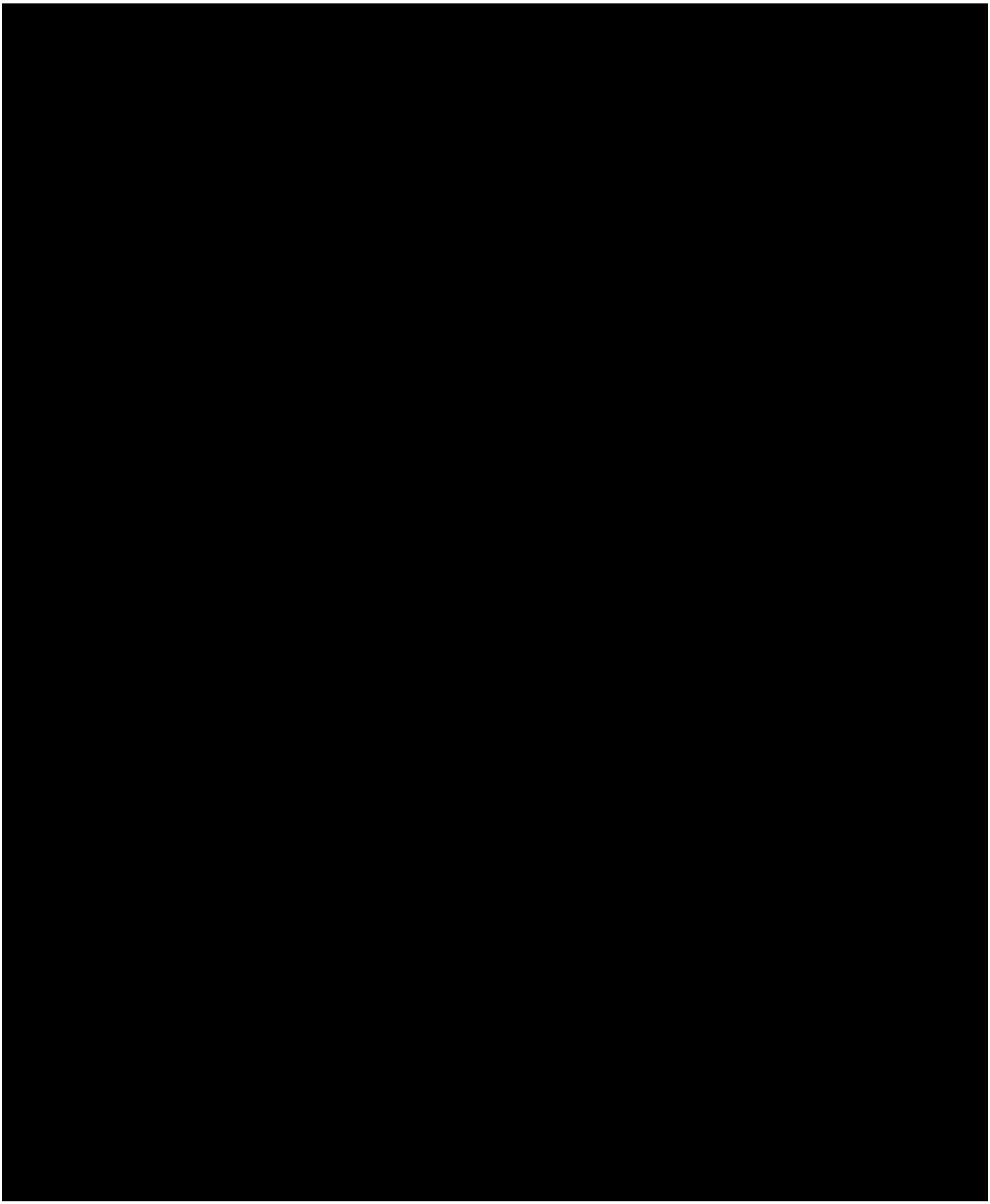


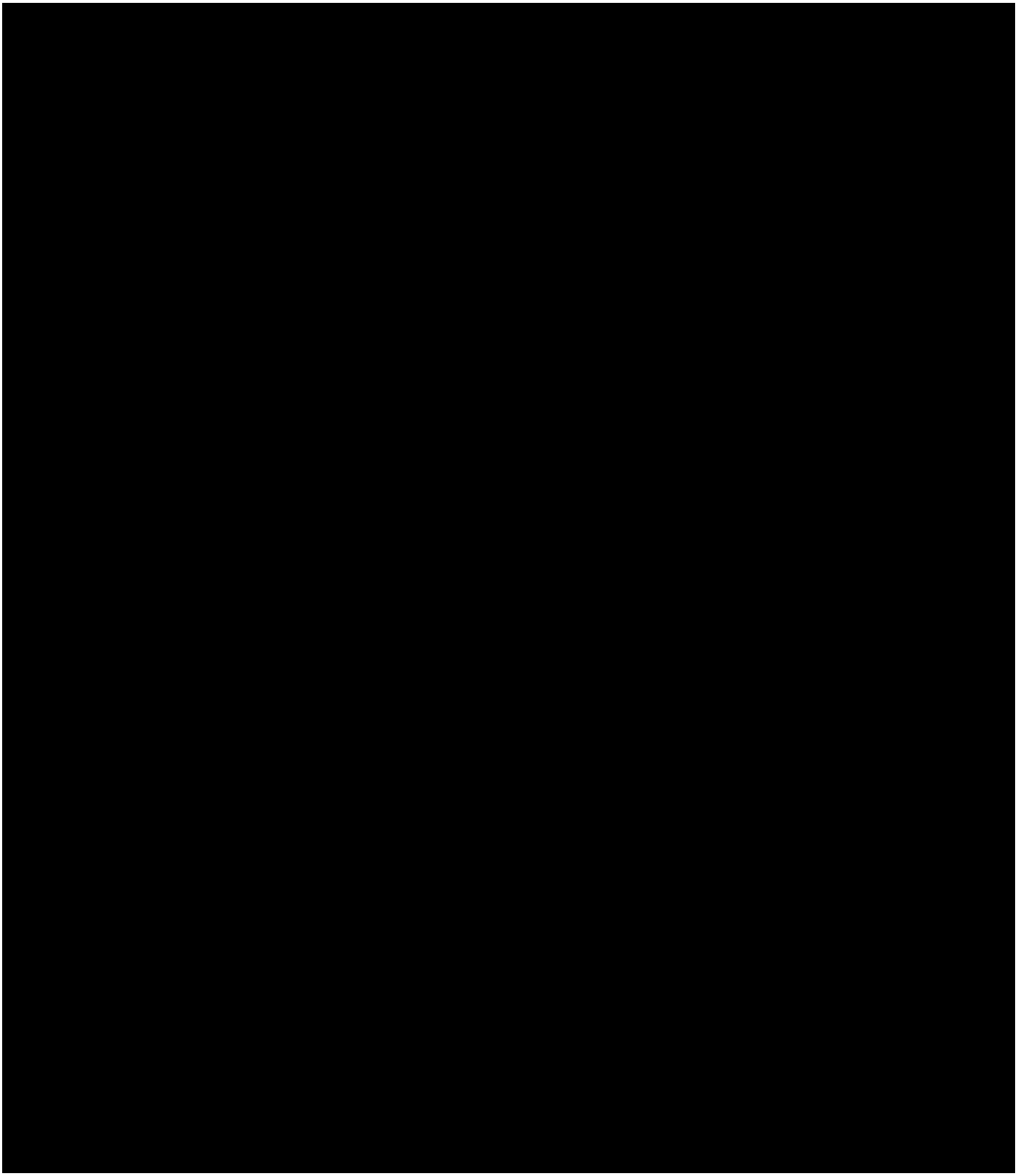


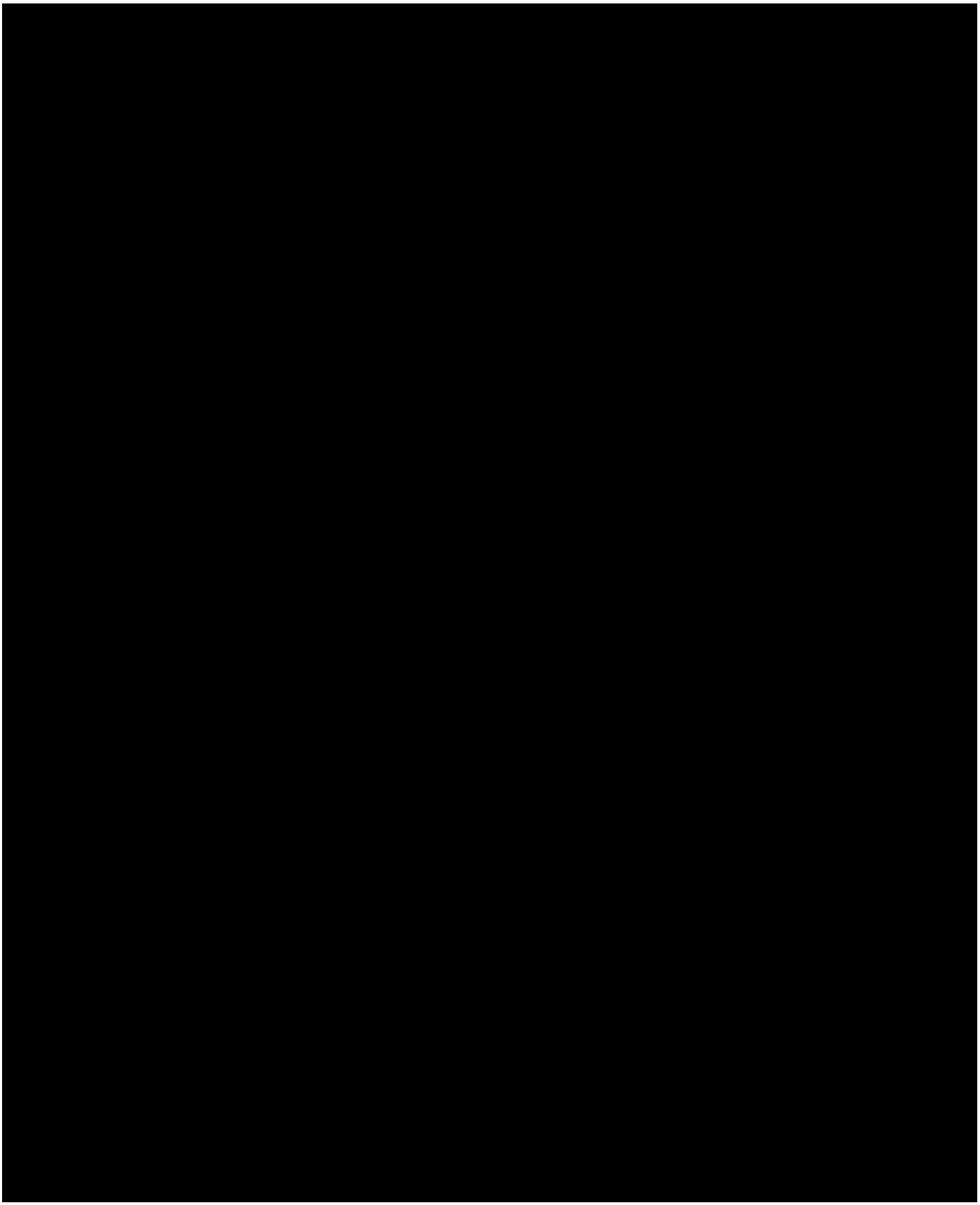
Crown Commercial

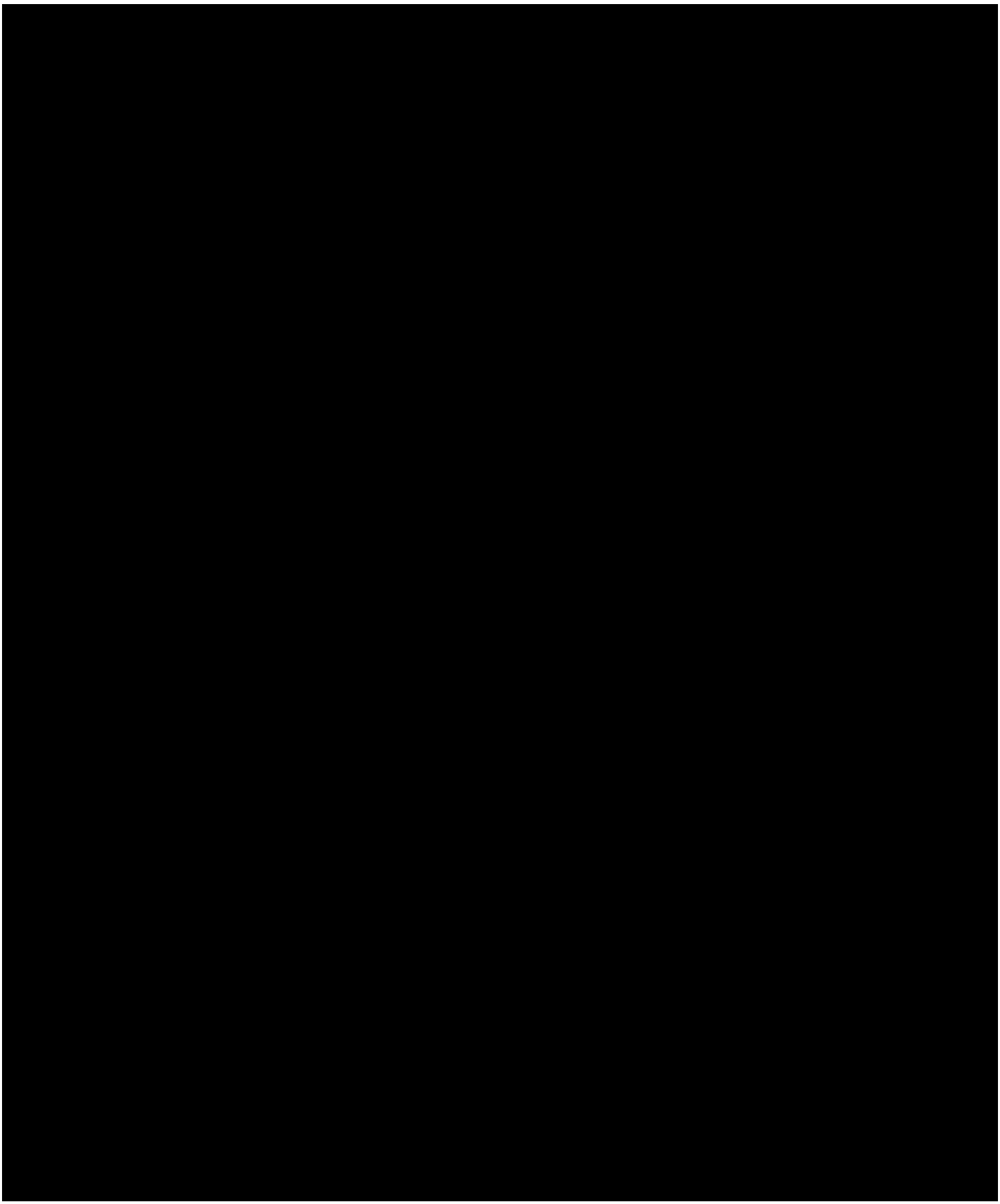






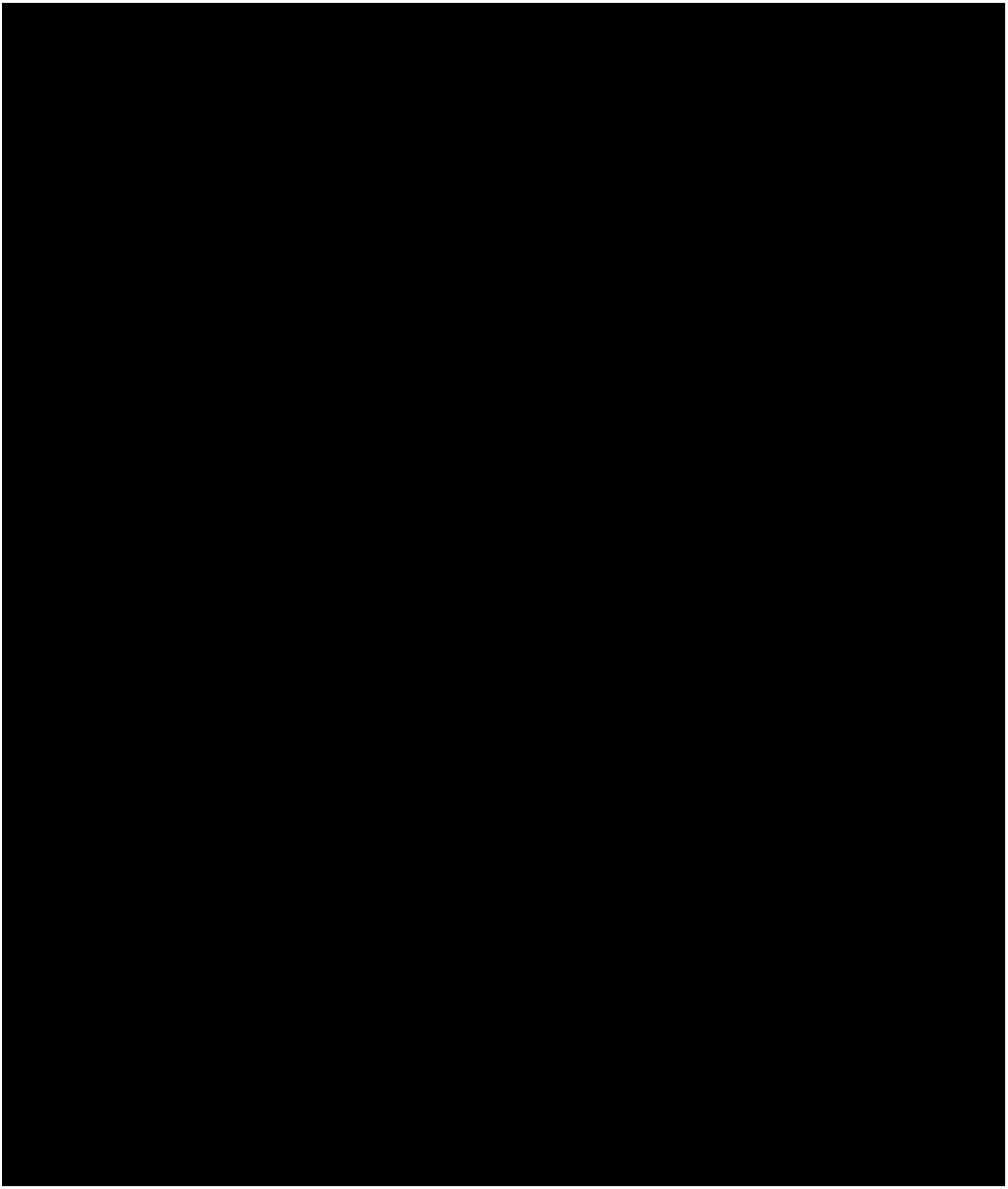




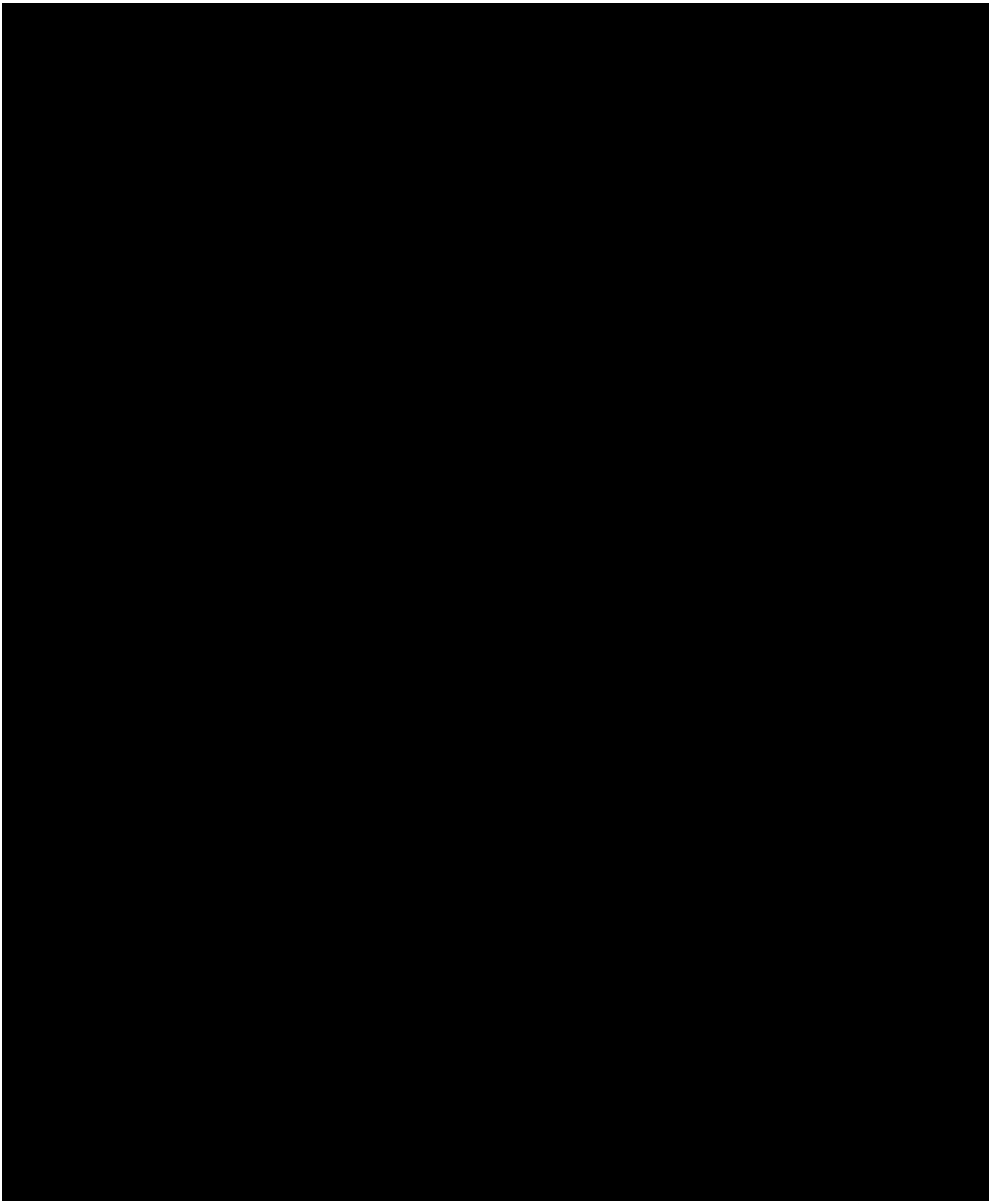


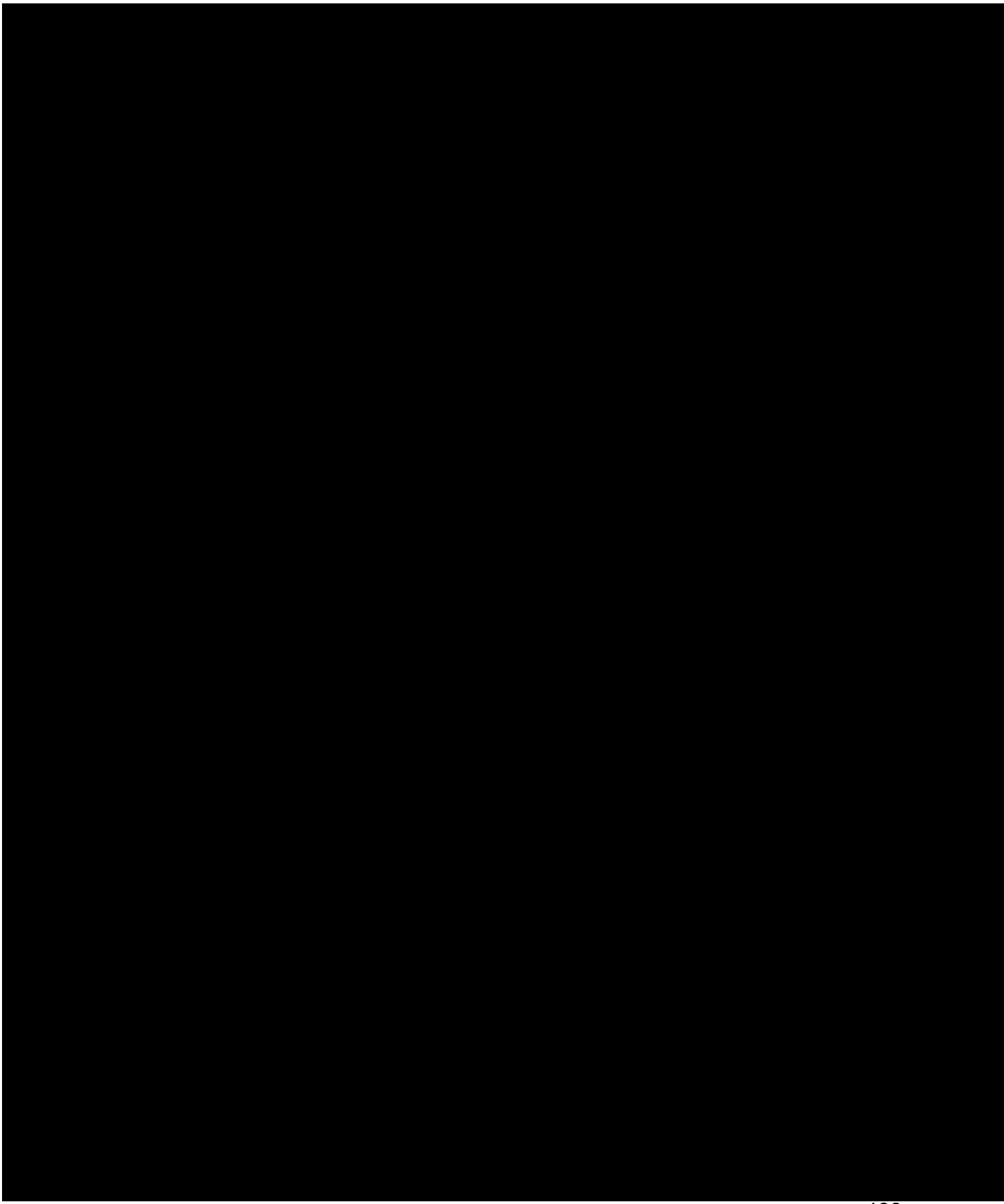
Crown
Commercial

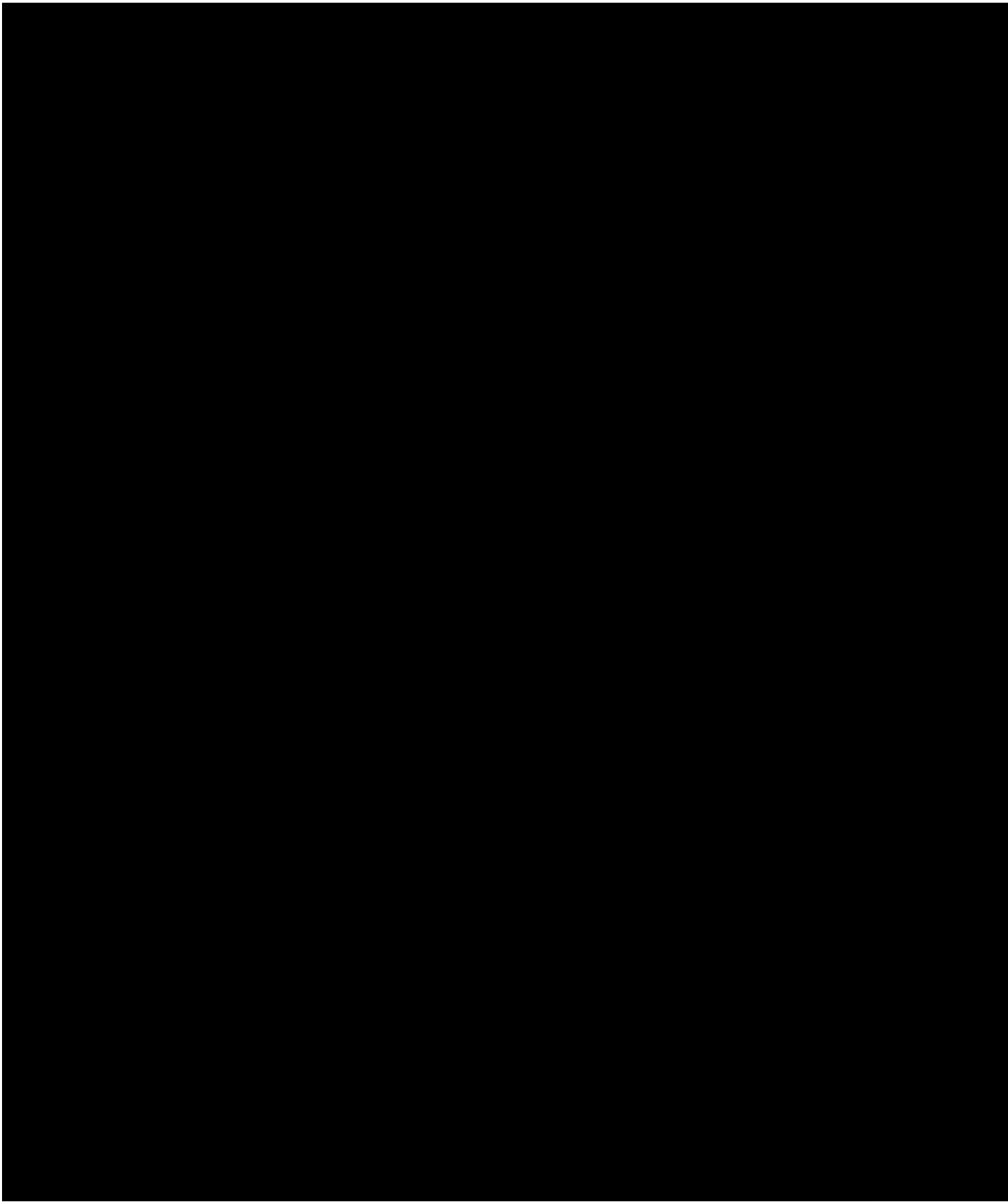
[redacted]

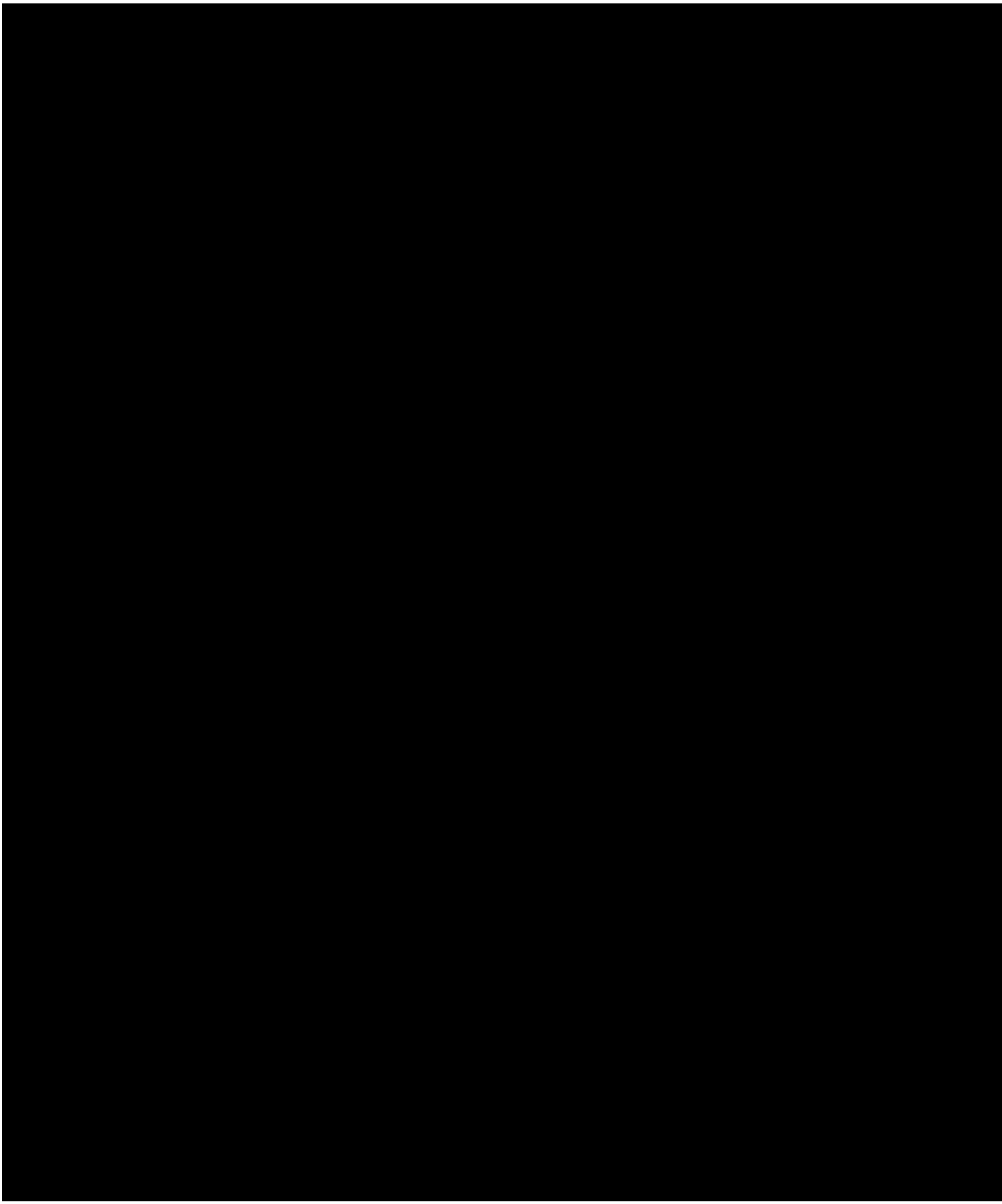


Crown
Commercial





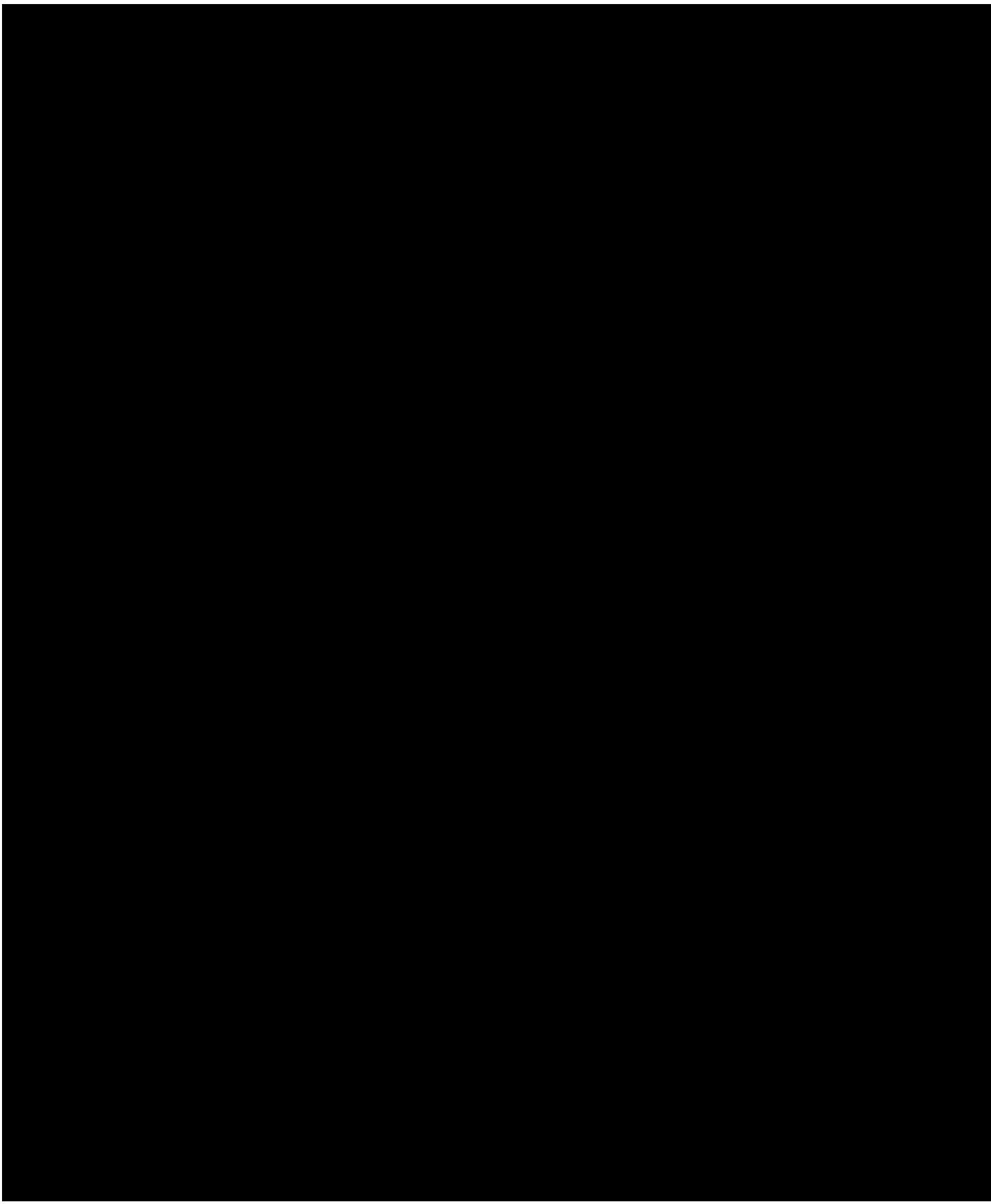


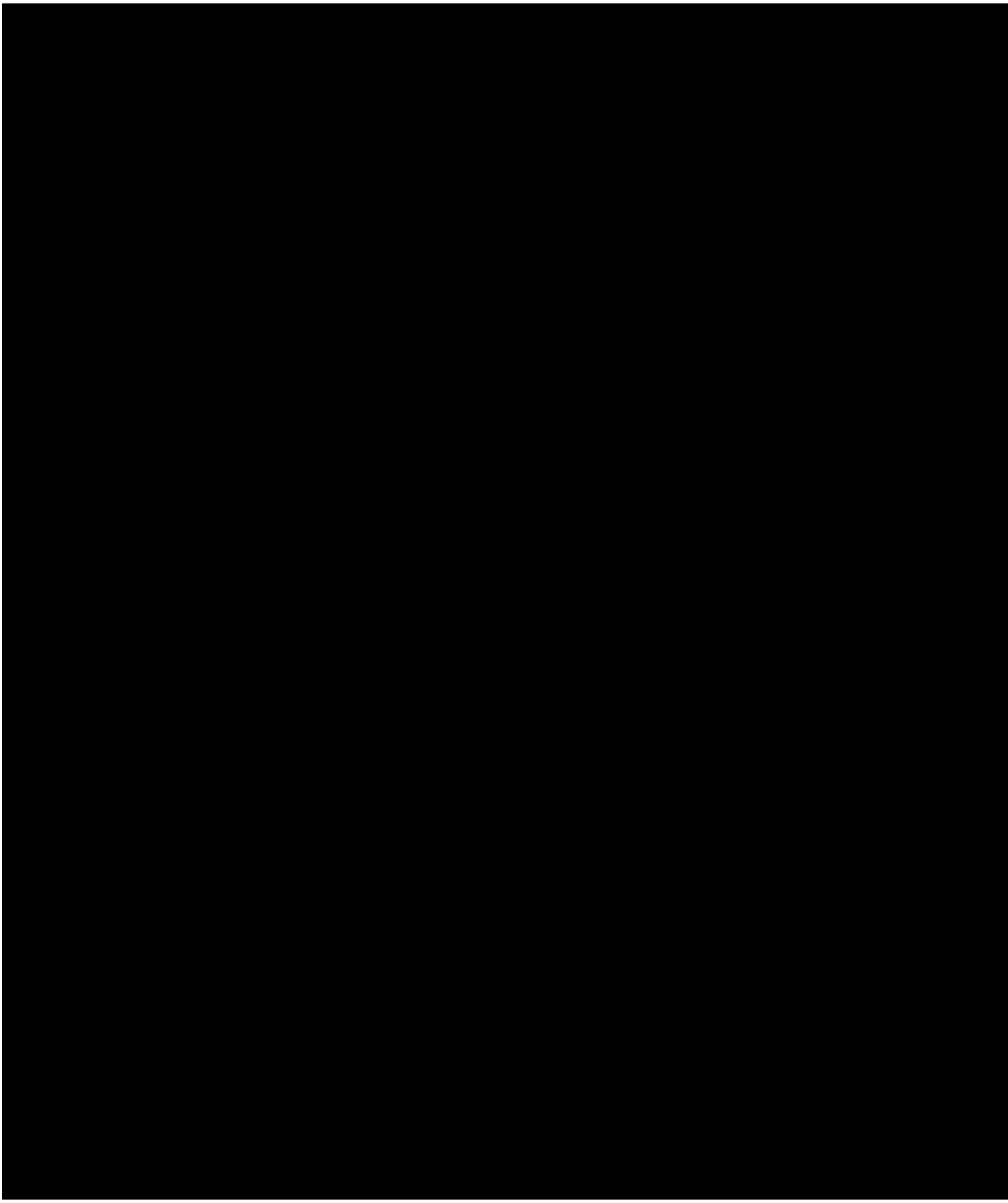


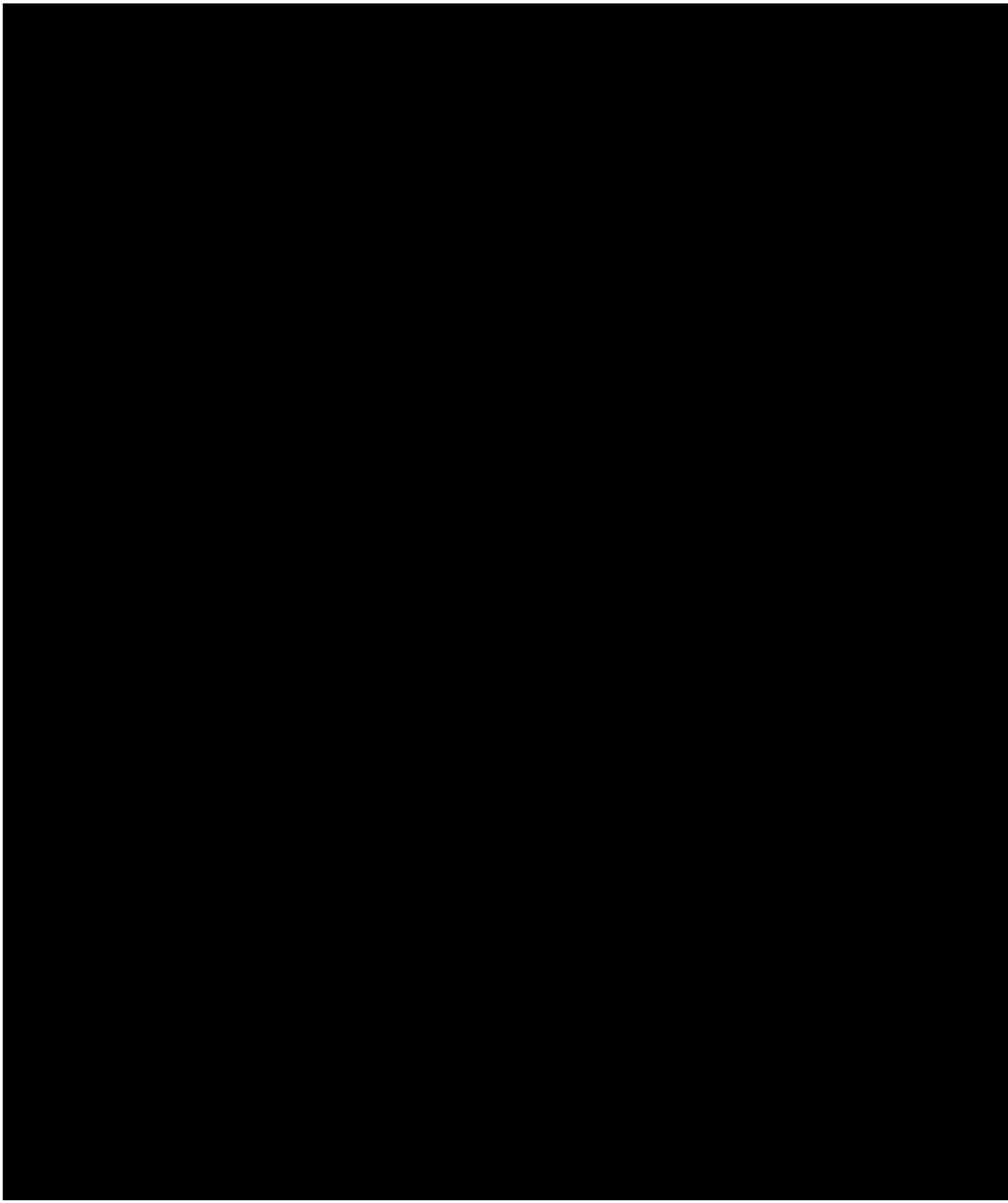
Crown Commercial

Crown
Commercial

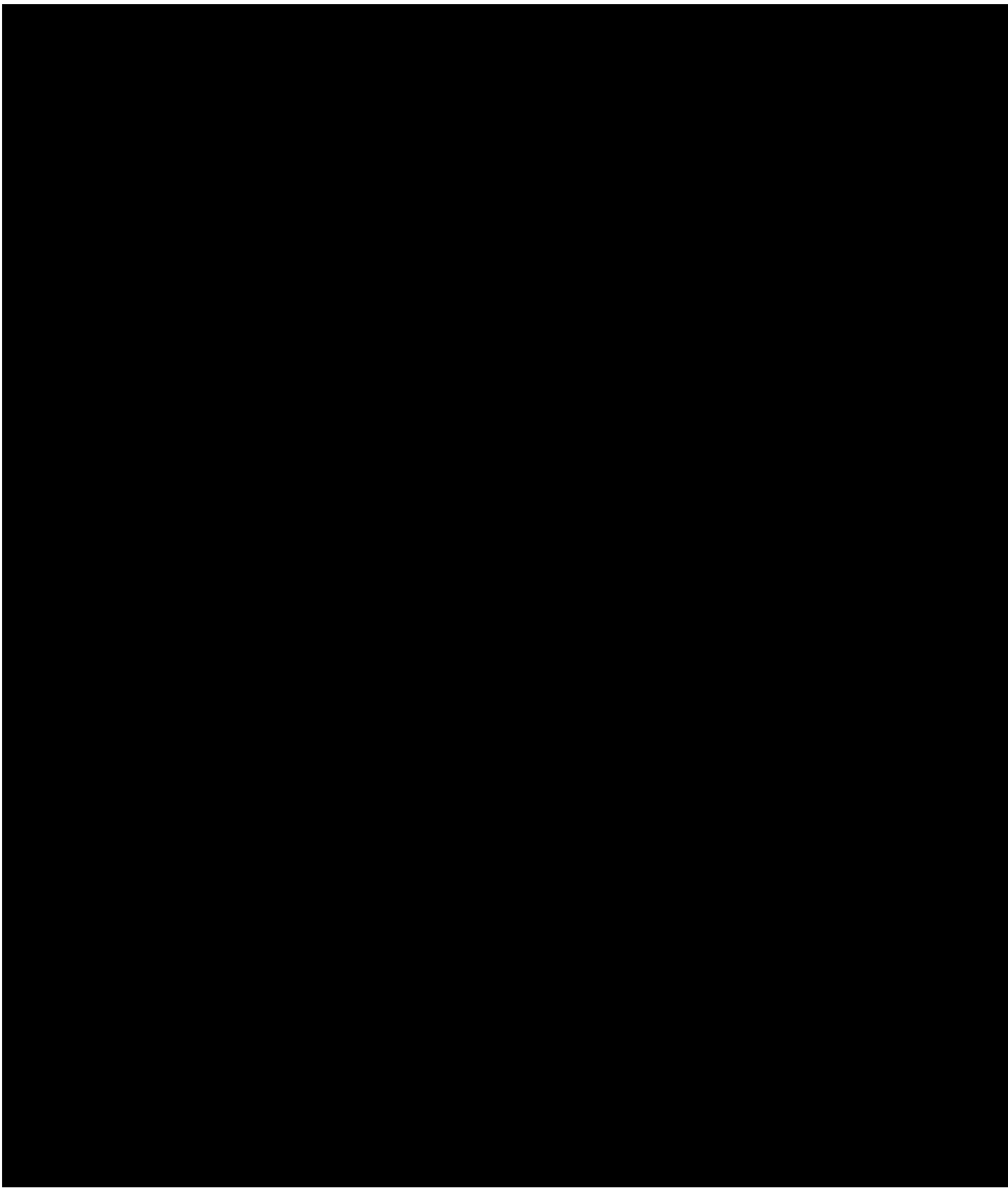
[redacted]

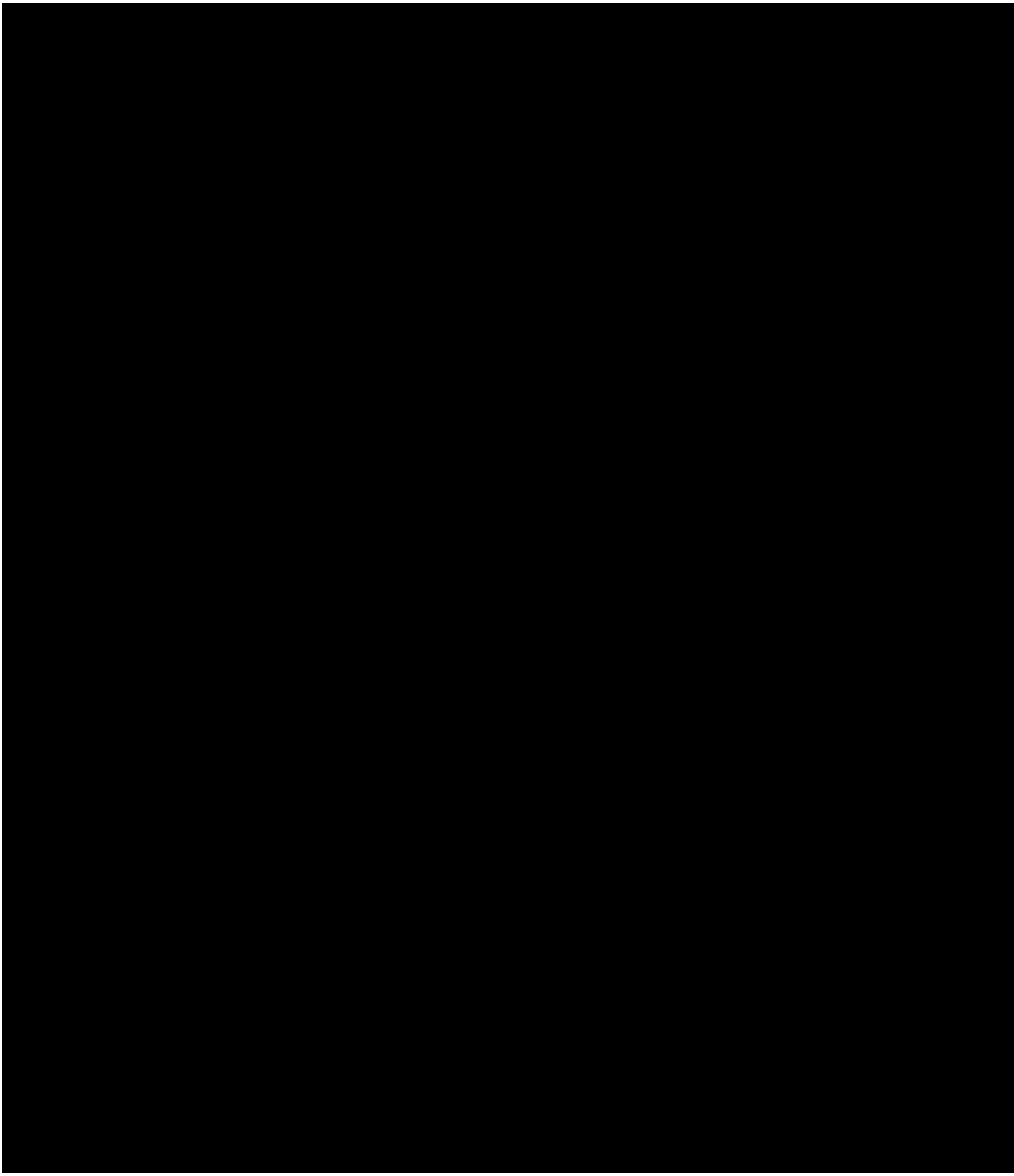




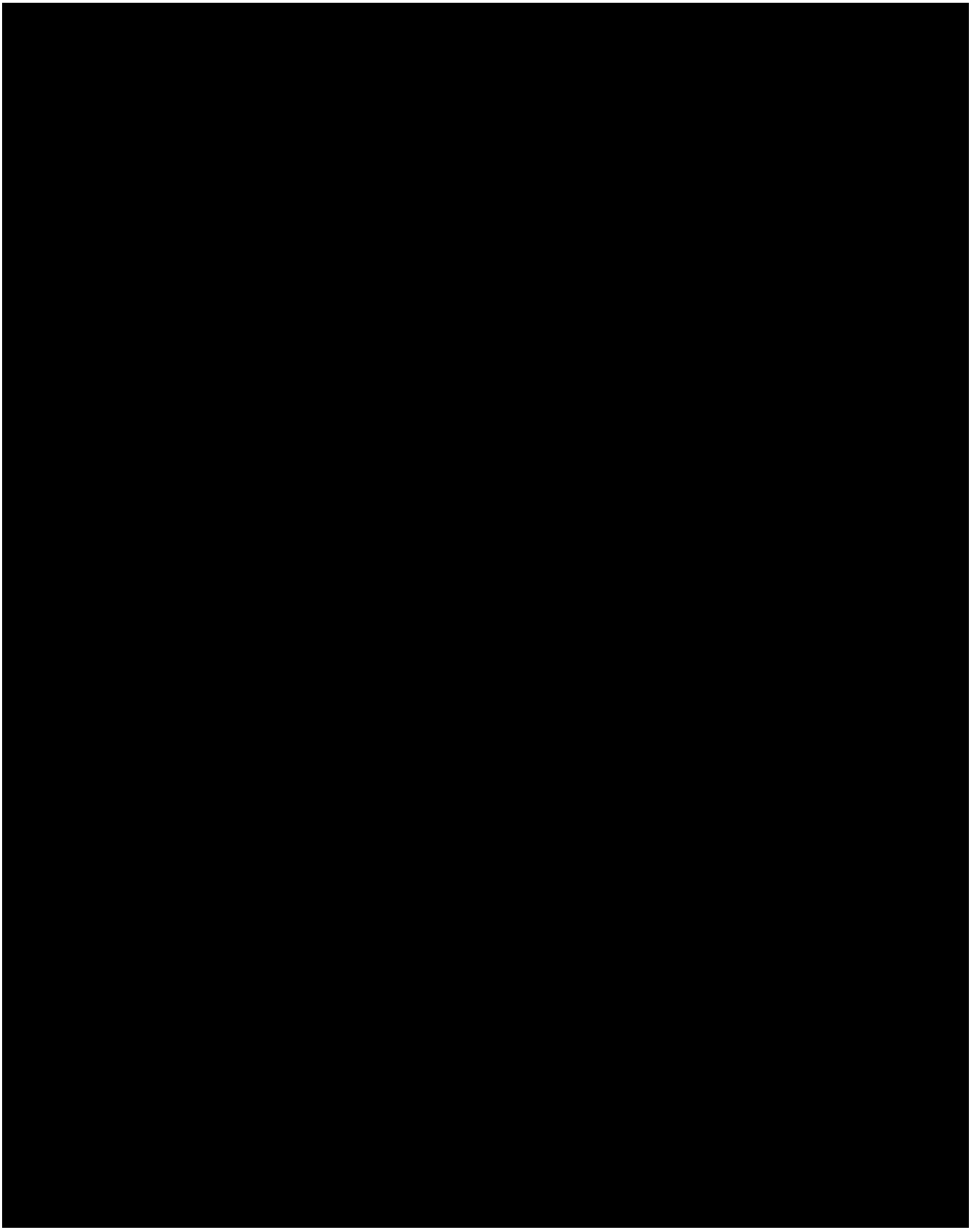


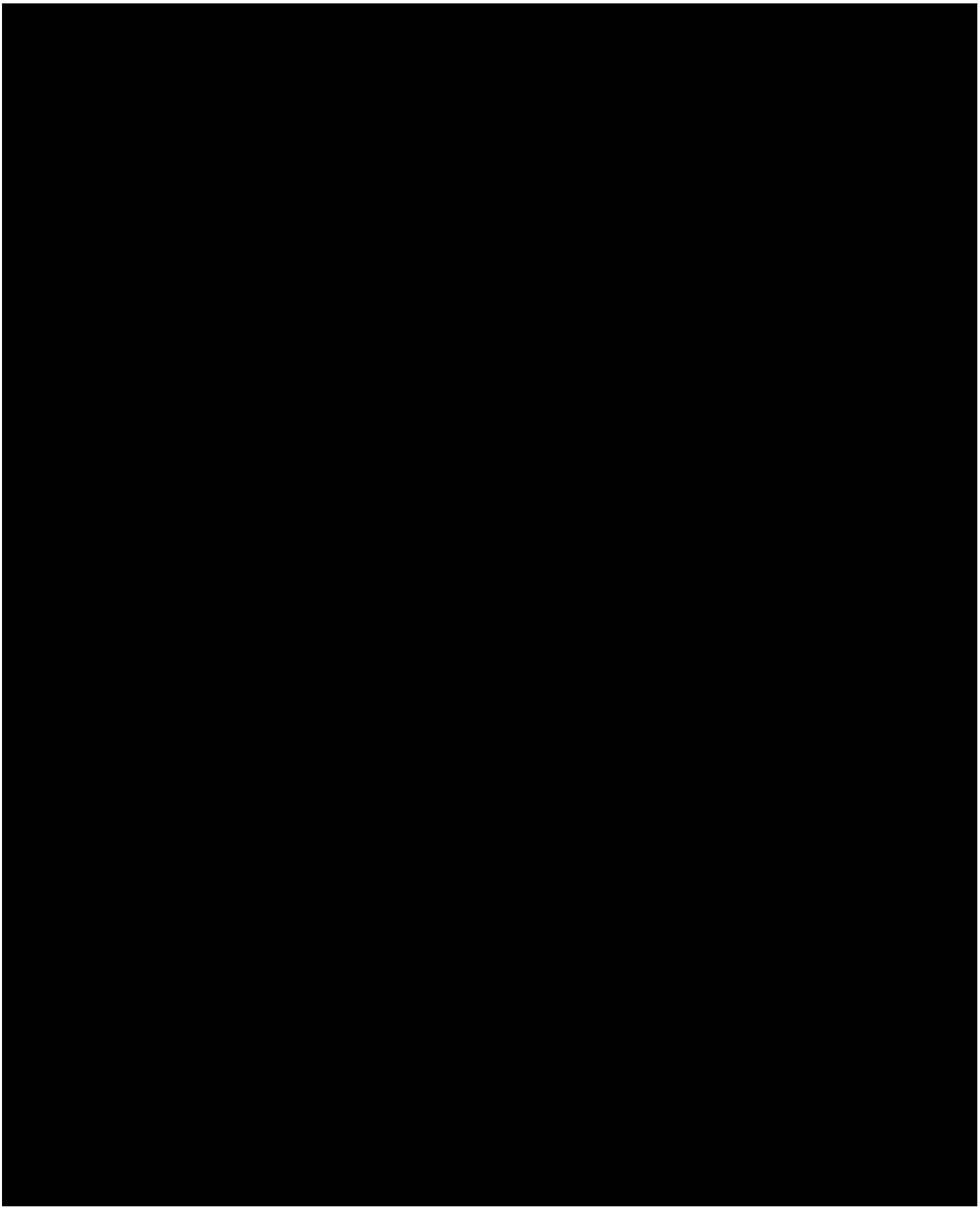
Crown Commercial





Crown
Commercial





Crown Commercial

ANNEX B – Work Package Template

FS430635
Request for Quotation

Work Package Number:
Work Package Title:
Available Budget: £
Supplier Name: Methods Business & Digital Technology
Specification of requirements – (to be completed by FSA)
Supplier response – please provide a detailed methodology of how you will deliver the requirements
Delivery timescales – Please provide a detailed plan of when you will deliver the specified outcomes
Please detail any assumptions you have made
Please detail any identified risks and your proposed mitigation measures
Costings – Please provide a detailed breakdown of all costs to deliver the specified requirements
GDPR - Processing, Personal Data and Data Subjects (where not covered by overarching contract)

Description	Details
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with the overarching contract, (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:

	• ***[Insert** the scope of Personal Data for which the purposes and means of the Processing by the Supplier is determined by the Buyer*
Duration of the Processing	*[Clearly set out the duration of the Processing including dates]*
Nature and purposes of the Processing	*[Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*[Describe how long the data will be retained for, how it be returned or destroyed]*
Completed by:	

Crown Commercial

Date:
Date quotation accepted by FSA:
Work Package start date:
This quotation for the above mentioned Work Package has been agreed between the Food Standards Agency and the Supplier under the terms and conditions of the contract FS430635 – Cloud Infrastructure Management **Signed on behalf of the FSA** Name: Signature: ---------- Position: Date: **Signed on behalf of the Supplier** Name: Signature: ---------- Position: Date: