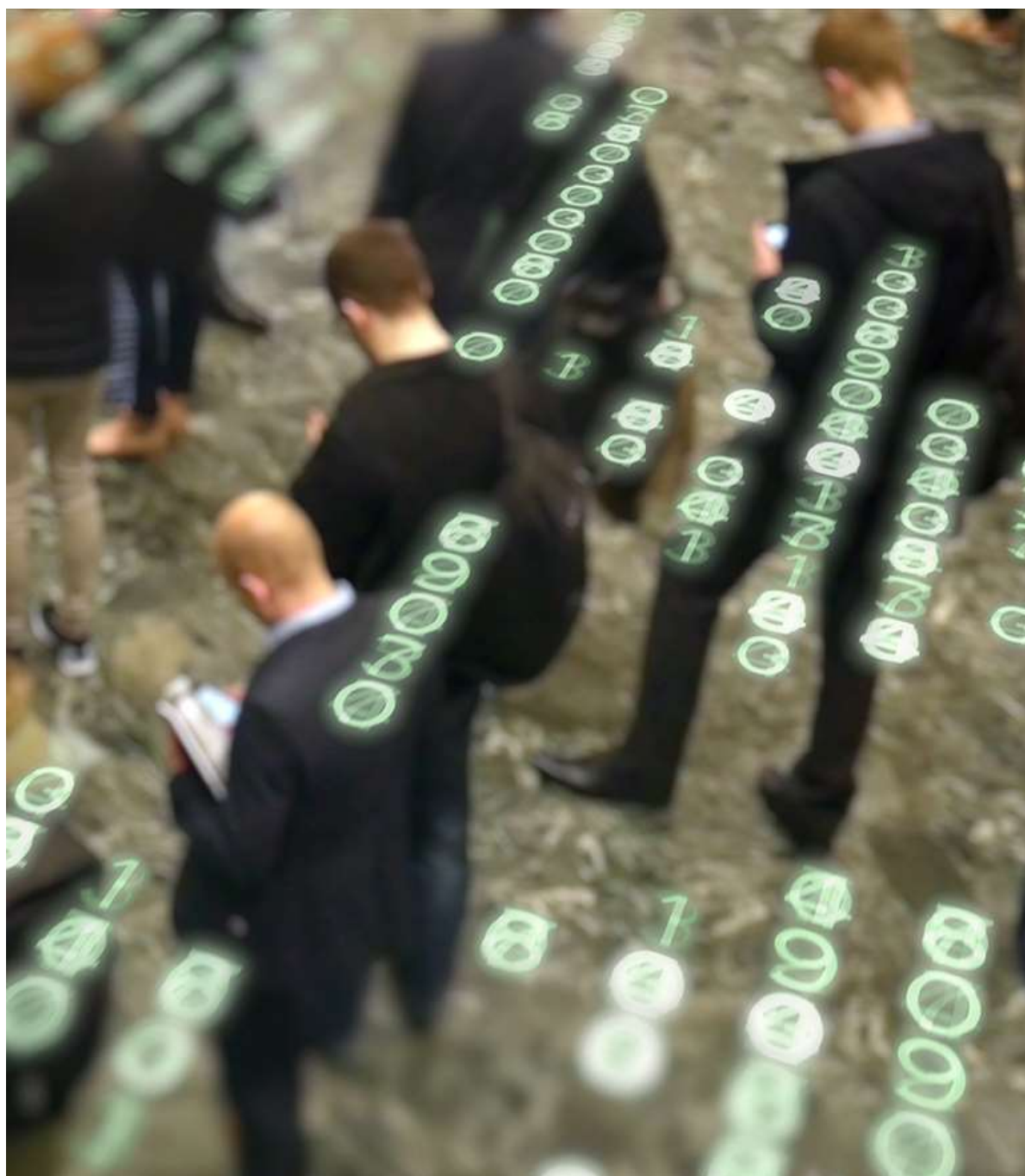


Privacy Impact Assessment - Central Credit Register

May 2018

Version 2.0



DOCUMENT APPROVAL

Version	Role	Name	Title	Signature	Date
v 0 x	<i>Reviewer / Approver</i>	<i>AN Other</i>	<i>Title, Organization</i>	<i>Signature</i>	<i>DD/MM/YYYY</i>

TABLE OF CONTENTS

1	Introduction	7
1.1	Introduction and Background to PIA	7
1.2	Purpose, Scope and Approach of PIA	10
1.3	Structure of the PIA	11
1.4	Acknowledgements and Use of This Report	12
2	Findings Summary	13
2.1	Introduction	13
2.2	The Inclusion of the Personal Public Service Number (PPSN)	13
2.3	Positioning of the PIA in the Development and Change Process	16
2.4	Privacy Protection Measures Within the Design	16
2.5	Findings	17
2.6	Privacy Principle: Legal Basis	17
2.7	Privacy Principle: Necessity	18
2.8	Privacy Principle: Proportionality	19
2.9	Privacy Principle: Subsidiarity of Data Processing	21
2.10	Privacy Principle: Responsibility	22
2.11	Privacy Principle: Limitation of Data Collection	23
2.12	Privacy Principle: Purpose Limitation / Limitation of Use of Personal Data	24
2.13	Privacy Principle: Data Quality	29
2.14	Privacy Principle: Security of Data	31
2.15	Privacy Principle: Transparency	36
2.16	Privacy Principle: Rights of Individuals	37
2.17	Additional Items for Consideration	38
3	Description of the CCR System, Processes and Dataflows	41
3.1	Introduction to the CCR System	41
3.2	Objectives of the CCR Data Processing System	57
3.3	Design Constraints for the CCR System	57
3.4	CCR Data Model	57
	Appendix I: Detailed CCR Data Model	59
	Appendix II: Universal Privacy Principles	84
	Appendix III: Universal Privacy Risks	86
	Appendix IV: Relevant Legislation, Regulations and Reference Material	88

Glossary of Terms

The following table identifies the terms referred to in this PIA. Nothing in this glossary supersedes any terms defined in the Credit Reporting Act, Data Protection Acts, or Central Bank Regulations.

Anonymization	The process of irreversibly turning personal data into a form which prevents identification of the data subjects.
CCR ID	Central Credit Register Identifier number. The unique number used on the CCR to identify each CIS.
CDMS	Customer Data Management System. Secondary database used by the CCR to manage CIS contact and engagement.
Central Bank of Ireland (CBI)	The single unitary body which is responsible for both central banking and financial regulation in Ireland.
Central Credit Register (CCR)	A database of personal and credit information established by the CBI under the Credit Reporting Act 2013.
Credit	A loan, deferred payment or other form of financial accommodation provided to a CIS by a CIP.
Credit Agreement	An agreement made between a CIP and another person (CIS) for the provision of credit for the other person.
Credit Application	An application for the provision of credit made to a CIP and completed in accordance with the application processes of the CIP by a CIS.
Credit Information Provider (CIP)	Also known as a lender. This is an entity which provides credit to a CIS. They can be a regulated financial services provider, NAMA, a local authority or any person who provides credit facilities (except a pawnbroker, the CBI or other central banks).
Credit Information Subject (CIS)	Also known as a borrower. This is a person who has made a credit application to a CIP, or entered into a credit agreement for the provision of credit, or is a guarantor.
Credit Reporting Act	The Credit Reporting Act is legislation, published in 2013, which provides for the establishment, maintenance and operation of a Central Credit Register by the Central Bank of Ireland.
Credit Score	Relating to a CIS, it is a value assigned to a CIS on the basis on the information on the CCR. It is used in order to indicate the level of risk of the CIS defaulting on financial obligations.
CRIF	CRIF is an Italian company that specialises in credit information systems. They operate in Europe, America, Africa and Asia and provide credit bureau services in other countries. CRIF Ireland Limited was selected by CBI to be the operators of the CCR following an open procurement process.
Data Breach	An incident where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration.
Data Controller	A person or legal person who controls the content of the data and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Flow	A graphical representation of the flow of information or data through a system.
Data Processing	Performing any operation or set of operations (manual or automated) on information or data including: obtaining, recording, keeping, collecting, organising, storing, altering, adapting, retrieving, consulting, using, disclosing, transmitting, disseminating, aligning, combining, blocking, erasing, destroying etc.
Data Processor	A person or legal person that holds or processes the data on behalf of the data controller (this does not include an employee of a data controller who processes such data in the course of his/her employment)

Data Protection Act	The Data Protection Act is legislation, published in 1988, which mandates for the protection of personal data. It was revised in by the Data Protection Amendment Act 2003 and is based on EU Directive 95/46.
Data Quality	The level of quality of data. High quality data can be considered fit for purpose, and can be used to make decisions.
Data Subject Access Request (DSAR)	Under section 4 of the Data Protection Acts, 1988 and 2003, a data subject has a right to obtain a copy, clearly explained, of any information relating to them kept on computer or in a structured manual filing system, by any person or organization, regardless of when the data was created. To exercise this right, a subject must make a data subject access request to the data controller.
Encryption	A technical process to convert data into an unreadable format which cannot be unconverted by an unauthorised individual.
Existing Loans	Existing credit agreements made between a CIS and a CIP before the establishment and operation of the CCR.
Firewall	A network device used to prevent unauthorised users from accessing networks, systems and data.
Identity Fraud	The fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.
Information Security Management Systems	A systematic approach used in the management of sensitive information so that it will remain secure. The approach includes people, processes and IT systems.
ISO27001:2013	International security standard defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is part of a family of standards relating to information and cyber security. It defines a comprehensive set of controls based on best practice in information security. Superseded the legacy ISO27001:2005 version.
NAMA	National Asset Management Agency
Office of the Data Protection Commissioner (ODPC)	Established under the 1988 Data Protection Act, the ODPC is an independent body responsible for upholding the rights of individuals as set out under Irish data protection legislation. The Commissioner is appointed by Government.
Personal Public Service Number (PPSN)	The Personal Public Service Number is a unique reference number issued by the Department of Social Protection to individuals in the State. It used by an individual for accessing public services.
Privacy	A fundamental right of individuals to be left alone which is recognised by the Supreme Court, the High Court, and the EU Charter of Fundamental Rights.
Privacy Impact Assessment (PIA)	A tool which can help organizations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. It should help an organization to identify and reduce the privacy risks of a project.
Privacy Risk	The risks associated with intrusion into an individual's right to privacy.
Profiling	The process of construction and application of profiles generated by computerised data analysis. This involves the use of algorithms or other mathematical techniques that allow the discovery of patterns or correlations in large quantities of data, aggregated in databases.

Single Borrower View (SBV)	This is the consolidation of all credit agreements associated with individuals (CIS), including credit agreements to groups of individuals to provide a single view of all credit agreements for which a person is individually liable.
System Administrator	The individual whose role it is to manage the operation of an IT system, including maintenance, upkeep and configuration.
System Operator	Role held by an individual in the operation of an IT system in order to run the day to day operations of the system.

1 INTRODUCTION

1.1 INTRODUCTION AND BACKGROUND TO PIA

Under the terms of the EU/IMF Programme of Financial Support for Ireland in 2010, the Irish Government committed to establishing a legal framework that would facilitate the collection and centralization of financial information on borrowers. The legal framework was subsequently established through the Credit Reporting Act 2013 ("the Act").

The Act mandates the establishment of a Central Credit Register ("CCR") to be operated by the Central Bank of Ireland ("CBI"). The CBI has powers to make regulations setting out the detailed arrangements for the CCR, subject to consultation with the Office of the Data Protection Commissioner ("ODPC") and the consent of the Minister for Finance.

The Act makes it mandatory for Credit Information Providers ("CIPs") to report personal and credit information on Credit Information Subjects ("CISs") for all credit agreements (of at least €500), provided that either the CIS in question is an Irish resident at the time when the credit application or credit agreement was made, or the credit agreement is subject to Irish law. CIPs are obliged to check the CCR when considering credit applications of at least €2,000. These credit reporting obligations will apply to over 500 lenders, such as banks, credit unions, local authorities, NAMA, asset finance houses and moneylenders.

The CBI and CIPs will separately perform Data Controller roles, with each being responsible for the data processed within its environments. The CBI will take on the responsibility of Data Controller for the data stored in the CCR and, as part of this role, must ensure that the data protection rights of individuals are upheld. The CIPs will also take on the responsibility of Data Controller for the data that they provide to the CCR. Their obligations to the CISs under the Data Protection Acts¹ do not change under the Credit Reporting Act.

CRIF Ireland Limited will operate the CCR and be a Data Processor on behalf of the CBI, and the CBI will be responsible for ensuring that data is processed in line with the obligations outlined in the Data Protection Act and Credit Reporting Act. CRIF is an Italian company that specialises in credit information systems. CRIF operates in Europe, America, Africa and Asia and provides credit bureau services in other countries. CRIF was selected by CBI to be the operator of the CCR following a public procurement process.

1.1.1 Context and Purpose for the Privacy Impact Assessment

A Privacy Impact Assessment ("PIA") is a process of systematically considering the potential impact a project or proposed change will have on the privacy of individuals. By completing a PIA during a project it is possible to not only identify potential privacy issues but also to address such issues during the project lifecycle. Given this early consideration of privacy issues and the ability to address such issues during the project stage, PIA's enable privacy by design.

A PIA differs from an audit. Whilst audit conclusions are based on testing and evidence gathering, a PIA takes place during the project stage when there is not yet an operating environment to test. As such the findings of a PIA are based on discussion with relevant parties and the information that is provided by these parties. The PIA supports future audits by identifying potential privacy issues and the commitments made on how these will be addressed.

The fieldwork for this PIA took place during the period September to November 2015. The findings are based on the design as it was known and communicated to us at that point. If the design changes post the PIA or additional information becomes available, this should be reviewed and considered in the context of its possible impact on the PIA findings.

¹ Data Protection Act, 1988, Data Protection (Amendment) Act, 2003

A PIA considers privacy more broadly than just compliance with Data Protection legislation. Where a change or a project has the potential to impact an individual's privacy this is highlighted even where the planned change can be achieved without breaching Data Protection legislation.

A PIA was considered to be necessary for the CCR project as:

- The CCR will involve the collection of new information on individuals, including the potential collection of the PPSN which has a special status in Irish law;
- The Credit Reporting Act 2013 will compel CIPs to provide information to the CCR and an individual's consent is not required for this processing. It will no longer be possible for an individual to get a loan of €500 or more without agreeing to share their personal data with the CIP for onward transmission to the CCR;
- The CCR will result in an increased sharing of data across credit providers;
- A key objective of the CCR is to avoid individuals becoming over indebted and financially stressed. As such the CCR will contribute to decisions being made which could have a significant impact on individuals;
- The financial information about individuals that is required to support a functioning CCR is likely to raise privacy concerns and expectations.

The decision to undertake a PIA is an indication of the CBI's commitment to limit the impact on individual's privacy resulting from the establishment of the CCR.

1.1.2 Key Definitions

The following definitions, as per the Credit Reporting Act 2013², are used throughout this document:

- **CCR:** The Central Credit Register: A database of information established, maintained and operated by the Central Bank of Ireland. It may hold:
 - Personal information relating to a credit information subject
 - Credit information which relates to any credit application or credit agreement made by a credit information subject or any credit agreement in connection with which the credit information subject is a guarantor;
 - Details linking any credit information subject who has made a credit agreement for the provision of credit with any other credit information subject who has given a guarantee or indemnity in connection with the credit agreement or also has liabilities under the credit agreement, and; and
 - Credit scores and other analyses produced by the Bank in relation to a credit information subject.
 - General reports, analyses and statistics produced by the Bank from which credit information subjects cannot be identified
- **CIP:** Credit Information Provider: Any regulated financial services provider, NAMA, local authority, or any person who provides credit, other than any Central Bank of any territory or a pawnbroker.

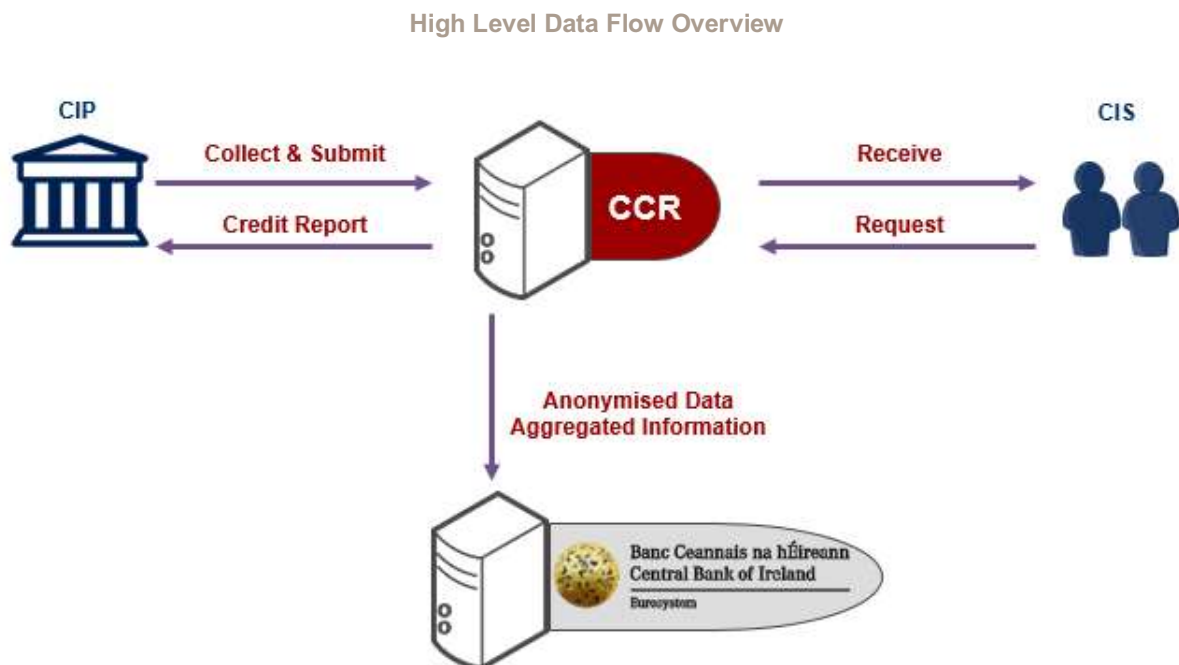
² Credit Reporting Act, 2013 sourced from: <http://www.irishstatutebook.ie/eli/2013/act/45/enacted/en/pdf>

- **CIS:** Credit Information Subject: a person who has made a credit application, has made a credit agreement for the provision of credit to the person, or is a guarantor.
- **CBI:** Central Bank of Ireland
- **Credit Score:** A numerical or alphanumeric value assigned to the CIS, on the basis of information on the CCR relating to the CIS, to indicate the level of risk of the CIS defaulting on financial obligations. This is not being implemented as part of Phase 1 of the CCR.

Additionally, **CRIF Ireland Limited** is the third party who has been appointed by the CBI to operate the CCR on behalf of the CBI.

1.1.3 High Level Data Flows

The following high level data diagram depicts the flow of credit and personal information to and from the CCR:



1.1.4 Classification of the Data in the CCR

This PIA reviewed the data model in the period September to November 2015, and classified the data using the following categories. These categories were defined specifically for the purpose of the PIA within the context of the CCR and the Credit Reporting Act (2013):

- **NON-PERSONAL DATA**
 - Data which cannot be related to an individual (e.g. Branch Code; Contract Reference Date; Currency)
- **PERSONAL DATA – NORMAL**
 - Data which could be related to an individual but only when combined with more specific unique identifiers (e.g. Surname; Forename; Address; DOB; Role of CIS)

- **PERSONAL DATA – IDENTIFIERS**
 - Data which could uniquely identify an individual directly without any additional data (e.g. PPSN; Provider CIS No.)
- **PERSONAL DATA – FACILITY**
 - Data which describes the financial status, performance or otherwise of an individual, but cannot be related to that individual unless combined with Personal Data- Normal or – Identifiers. Data Subjects (CISs) may consider facility data to be more sensitive than the PPSN or other personal data once it is linked to them. There is an inherent sensitivity associated with financial data, financial performance data or data which may be perceived to cast someone in a negative light. (e.g. Contract Status; Restructured Flag; Number of payments past due)

1.2 PURPOSE, SCOPE AND APPROACH OF PIA

1.2.1 Purpose

The purpose of the PIA is to assess the impact that the introduction of the CCR will have on an individual CIS's privacy and to assist in the evaluation of potential solutions to those risks. It sets out recommendations to enhance the privacy of individuals by "design" – e.g. by using privacy enhancing technology to design privacy into the proposed solution.

1.2.2 Scope

The Central Bank plans to implement the CCR on a phased basis.

- Phase I will focus on collecting information relating to consumer credit. It is expected that CIPs will provide consumer data to the CCR from June 2017 onwards. The capacity of CIPs to deliver data of sufficient quality will influence when searching the database will become feasible, although this will need to be monitored as the project progresses.
- A second implementation phase will focus on reporting non-consumer credit (e.g. sole traders, partnerships, companies and other incorporated bodies). It is anticipated that this phase will go live by March 2018.

The scope of the PIA is limited to Phase I of the CCR.

Out of Scope

- CBI CCR project related privacy risks;
- Technology solutions within the CIPs or their outsourced third party technology providers;
- Activities that are not in scope for Phase 1 of the CCR but will be part of future phases, e.g. Phase 1 excludes: Guarantor Data, Sole Trader Data, Corporate Data, a number of CBI statistical fields, certain CIPs including: moneylenders, NAMA, banks with corporate finance only, local authorities.

1.2.3 Approach

Mazars has followed a six stage approach to develop and produce this Privacy Impact Assessment for the CBI.



- 1. Mobilization:** Established a core group of CBI and Mazars staff who have a common understanding of the engagement approach, deliverables, schedule and stakeholders.
- 2. Data Flows:** Desktop review of key information flows to and from the CCR to understand data elements and flows to support privacy risk identification within the context of Data Protection & Credit Reporting legislation.
- 3. Identify Risks:** Identification of privacy related risks associated with the establishment of the CCR in line with the Credit Reporting Act, 2013.
- 4. Privacy Solutions:** Review potential solutions and set out recommendations for managing identified privacy risks.
- 5. Reporting:** Prepare and document the Privacy Impact Assessment report.
- 6. Align Work Plan:** Alignment of the recommendations with and incorporate actions from PIA into overall CCR Project Plan.

1.2.4 PIA Stakeholders

The following parties and stakeholders were consulted as part of this PIA:

#	Name
1	CBI CCR Project Team
2	CBI Legal and Legal Compliance Divisions
3	CBI Internal Divisions
4	CRIF Ireland Limited
5	Representative group of CIPs (including Banks and Credit Unions)

In addition, feedback from consumer market research conducted by CBI CCR Project was considered by the PIA team.

1.3 STRUCTURE OF THE PIA

This document is set out in the following structure:

Chapter 1: Introduction:

Introduces the concept of a Privacy Impact Assessment, outlines the approach and principles against which the impact to an individual's privacy was assessed and clearly defines the scope boundaries of the assessment.

Chapter 2: Findings Summary and Privacy Principles

Summarises the primary findings identified by the PIA across the eleven generally accepted principles of privacy and identifies the extent to which the solution will diminish the privacy of individuals.

Chapter 3: Description of the System

Describes the CCR data processing solution which is being developed by CRIF for the CBI, identifies relevant stakeholders and outlines the data model employed.

1.4 ACKNOWLEDGEMENTS AND USE OF THIS REPORT

Mazars was engaged by the Central Bank to complete this PIA. Mazars assumes no responsibility in respect of, or arising out of, or in connection with the contents of this report to parties other than to CBI. If others choose to rely in any way on the contents of this report they do so entirely at their own risk.

Mazars

May 2018

2 FINDINGS SUMMARY

2.1 INTRODUCTION

In Ireland, the Data Protection Act (DPA) provides the legislative framework for the protection of “personal data”.

The processing (either digital or manual) of any personal data has a potentially negative impact on the personal lives of individuals and on their wellbeing. We have considered the potential negative impacts on an individual’s privacy that could result from the establishment of the CCR. While all of these privacy risks are captured in sections 2.5 to 2.16 of this document, we have included a specific section on PPSN below. This consolidates in one section all the PPSN related points that are distributed individually across sections 2.5 to 2.16.

2.2 THE INCLUSION OF THE PERSONAL PUBLIC SERVICE NUMBER (PPSN)

2.2.1 Context

The capture and use of an individual’s PPSN is restricted under law. Given the legal status of the PPSN, we have considered its proposed use in the CCR design independently from the other personal data elements which will be used within the CCR.

The CCR will take advantage of two techniques that are available to validate PPSNs:

1. PPSNs will be validated using an algorithm referred to as modulus 23 which utilises a check character to identify incorrectly entered digits;
2. PPSNs will be confirmed as being linked with the correct person through utilising a PPSN checking service which is being made available through the Department of Public Expenditure and Reform

2.2.2 PPSN Related Privacy Risks

The Credit Reporting Act 2013³ specifically allows for the use of the PPSN in the CCR, giving a legal basis for its collection. There are four specific privacy risks that we identified regarding the use of the PPSN:

- Profiling of individuals by the CIPs;
- Profiling of individuals by government agencies or State bodies;
- Theft of an individual’s PPSN to commit Social Welfare or tax fraud;
- Use of the PPSN to gain unauthorised access to data (“snooping”).

Profiling of individuals by the CIPs: *If the CCR mandates CIPs capture PPSN, this will result in PPSN being captured on all borrowers (€500 and over) in the State. Each CIP could then use the PPSN to profile individual CIPs within an institution using the PPSN as a unique identifier.*

Not all CIPs have solutions in place to provide a single customer view that enable profiling of individuals to take place. Where this is the case, the use of the PPSN in the CCR would provide an identifier that would be very useful to CIPs in building profiling solutions. Where CIPs are already in a

³ Act 2013 Part 2, Section 6. (6)

position to create a single customer view across their products, the risk of a CIP using the PPSN to profile CISs remains but is reduced.

If CISs were mandated to provide their PPSN to secure credit and the PPSN was subsequently used to profile the individual this would constitute using the PPSN for a purpose other than what it was provided for. As such this would be a breach of the individual's privacy.

However, profiling of a CIS using the PPSN is not legally permitted under the Credit Reporting Act. Given this and the requirement for the CIPs to comply with the Data Protection Acts, using the PPSN to profile a CIS would require the CIP to knowingly break the law. It is unlikely that an entity licensed or regulated by the CBI, such as a CIP, would knowingly design a technology solution that breaks the law.

Profiling of Individuals by Government Agencies or State Bodies: Where the PPSN is used in the CCR database it could potentially be used to profile individuals' interactions and behaviour with other agencies or bodies, e.g. Revenue Commissioners, Social Welfare etc.

There may be benefits to the State in being able to profile individuals' interactions and payments across multiple state bodies or agencies and the CCR, e.g. detecting a fraud. This type of profiling would have the benefit to society of detecting crime. However, it would be a breach of the privacy principle of only using personal data for the purposes it was provided. This breach would impact not just criminals but all CISs.

At time of writing, we understand that this risk is theoretical only, i.e. there is no legislation in place that would allow sharing of the CCR data with other state bodies or agencies.

Additional comment on profiling: We recognise that the CCR itself profiles CIS's behaviour across multiple institutions over a period of years and provides information on this to CIPs. This is not a risk of the CCR, it is the purpose of the CCR and the explicit reason for capturing the CIS personal data. As such, profiling within the CCR is consistent with the privacy principles and data protection.

Social Welfare or tax fraud: There is a risk that the State could be defrauded through the unauthorised disclosure and use of a PPSN to claim social welfare benefits or tax credits.

There are known instances where individuals have used another person's PPSN to fraudulently claim social welfare benefits or tax credits in another person's name. For either of these frauds to be successful the legitimate owner of the PPSN cannot also be claiming the same benefits or credits.

Given this, it is much more likely that people committing a fraud will use the inactive PPSN number of an individual who is not residing in Ireland (there are in excess of 7m PPSNs in a country with a population of 4.6m people⁴).

In addition, the Department of Social Protection is undertaking the SAFE 2 project to address known risks associated with misuse of the PPSN. As part of this project the Department is in the process of rolling out physical public services cards to all welfare claimants. Access to social welfare services will be reliant on each claimant having a public services card which includes photo identification, so access to a PPSN will no longer be sufficient on its own to access social welfare payments.

Snooping: There is a risk that the PPSN could be used by private investigators or others for investigations into a CIS⁵ i.e. by pretending to be the target individual and using the PPSN with other personal data to get information on the target individual from the Department of Social Protection. The risk exists that the PPSN could be sourced from a CIP or the CCR directly.

We note that the Office of the Revenue Commissioners is aware of the general risks associated with the PPSN and has issued guidance to financial institutions which include restrictions on the use of

⁴ PPSN statistics sourced from: <http://debates.oireachtas.ie/dail/2011/09/14/00234.asp>

⁵ Sourced from: <https://www.dataprotection.ie/docs/6-10-14-data-protection-commissioner-welcomes-outcome-of-prosecution-proceedings-against-private-investigators-/1459.htm>

PPSN⁶. This guidance requires that PPSN should not be used as part of search criteria and should be masked from users except in specific circumstances (e.g. opening an account).

We recommend the application of the Revenue recommended controls in the CIPs. In addition, application of these controls within the CCR should be considered. We understand that it may not be practical to apply the controls within the CCR and note that additional controls are in place i.e. CCR staff will sign up to additional security and confidentiality undertakings as part of their employment contracts. These clauses would make it possible, in certain instances, to hold a CCR staff member accountable for breach of personal data security.

2.2.3 PPSN Related Privacy benefits to the individual

While the use of the PPSN within the CCR will introduce risks to the privacy of the CIS, it will also provide some additional privacy protection.

Privacy and Data Protection principles require that data is of a high quality, including being accurate. In the absence of the PPSN, the ability to match an individual to all of their loans will be reduced. This could negatively impact CISs who have consistently paid their loans on time and have a good credit history.

The ability of the CCR to achieve accurate matching is more heavily reliant on PPSN than on other personal data. As such, the PPSN may be used to address privacy rights through the accurate identification and matching of CISs.

Effectiveness of the PPSN in supporting matching

We recognise that the CCR is being established with a view to achieving societal benefits:

- Providing lenders with more comprehensive analysis of borrowers' creditworthiness through the single borrower view (SBV);
- Equipping borrowers with information on their financial profile and helping them avoid over indebtedness;
- Giving the Central Bank better insight into financial markets and supporting several functions e.g. prudential supervision, statistics, financial stability.

Without using the PPSN, the CCR's ability to achieve these societal benefits would reduce, as the accuracy of matching would be reduced.

2.2.4 Conclusion

There are risks associated with using the PPSN for the CCR which, if they materialise, would impact on an individual's privacy. However, these risks are reduced by:

- Legislation in the case of profiling;
- The likelihood of prosecution if using an active PPSN in the case of fraud;
- Applying Revenue guidelines in the case of snooping within the CIP or possibly the CCR;
- Strong privacy and security clauses in staff contracts in the case of the CCR.

⁶ Revenue guidance sourced from: <http://www.revenue.ie/en/practitioner/law/notes-for-guidance/financial-institutions/index.html>

We also recognise that using the PPSN supports a more effective CCR and more accurate matching of data. This is a benefit to society and to the CISs that have consistently repaid their loans and consequently have a good credit history.

Given the risks, controls and benefits of using the PPSN, the CBI may reasonably conclude that the use of PPSN for meeting the CCR needs is proportional to the risks.

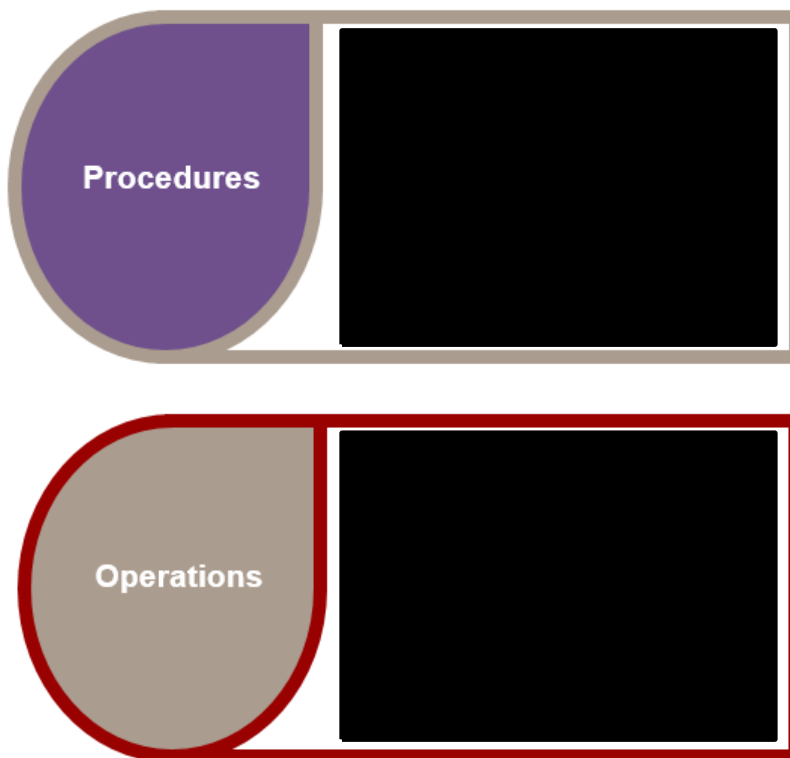
2.3 POSITIONING OF THE PIA IN THE DEVELOPMENT AND CHANGE PROCESS

The PIA exercise was undertaken during the design stage of CBI's CCR project and therefore needs to be considered in light of the ongoing and changing development process for the delivery of the project. Phase I of the CCR is projected to go live in June 2017, and detailed specification of requirements are being finalised at the time of writing. Therefore, not all design decisions have been made at the time the PIA was undertaken.

However, we understand that the CBI will consider the findings of the PIA when finalising design questions. As such both the CBI and its third party outsourced provider will be better positioned to make informed design decisions while upholding individual's right of privacy.

2.4 PRIVACY PROTECTION MEASURES WITHIN THE DESIGN

A number of privacy protection measures are being built into the design of the CCR. The following positive privacy measures were being established or are planned for implementation at the time this PIA was undertaken:





2.5 FINDINGS

Mazars has been conducting PIAs for the last ten years. Over this period, we have developed a set of privacy principles. These principles are consistent with the OECD, EU and national legislation, including the Irish Data Protection Acts. In addition, they reflect available best practice guidelines.

We have captured the privacy risks associated with the CCR under each of the 11 privacy principles listed below.

2.5.1 Privacy Principles



2.6 PRIVACY PRINCIPLE: LEGAL BASIS

2.6.1 Situation

The Credit Reporting Act 2013 provides the legal mandate for the CBI to establish and operate the CCR. The Act provides the CBI with the full legal authority to instruct CIPs to provide credit and personal information for the purposes of populating a central database of credit intelligence.

The following additional Irish legislation, EU Directives and future regulations relating to the right to privacy and protection of personal information also need to be considered within the delivery and operation of the CCR:

- The Data Protection Acts (1988 and 2003)⁷ mandate the protection of personal information relating to individuals and obliges Data Controllers to ensure the security of personal data they collect and process.
- The EU Data Protection Directive⁸ regulates for the processing of personal data within the European Union.
- Draft EU General Data Protection Regulation⁹.

2.6.2 Findings

The Credit Reporting Act, 2013 sets out a clear legal basis for collection and processing of personal and credit information on the CCR. It lays down rules for collection, access, use and retention of personal data, including the PPSN and credit information, together with obligations to inform CISs, to allow them access their records and to seek rectification of errors.

CBI Management Response

None Required

2.7 PRIVACY PRINCIPLE: NECESSITY

2.7.1 Situation

The need to establish a centralised repository of personal data and credit data relating to individuals is directly related to the Irish Government's agreement to terms and conditions of the EU/IMF Economic Adjustment Programme for Ireland.

Under the programme of external financial assistance, the Government committed to develop a legal framework that would facilitate the collection and centralization of financial information on CISs in order to produce a Single Borrower View (SBV). The CCR will provide a Single Borrower View (SBV) of all credit agreements relating to an individual CIS who has obtained credit from CIPs¹⁰:

2.7.2 Findings

The Credit Reporting Act, 2013 arose from recommendations of the Report of the Interagency Working Group on Credit Histories¹¹ and formed part of Ireland's commitments under the EU/IMF Programme of Financial Support for Ireland.

CBI Management Response

None required

⁷ Data Protection Act, 1988, Data Protection (Amendment) Act, 2003

⁸ EU Data Protection Directive 95/46/EC.

⁹ Proposal for New EU General Data Protection Regulation, sourced from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

¹⁰ CCR FAQ paper, sourced from: <http://www.centralbank.ie/press-area/press-releases/Documents/Central%20Credit%20Register%20-%20FAQs.pdf>

¹¹ Sourced from: <http://www.finance.gov.ie/sites/default/files/Report%20of%20the%20Inter-Agency%20Working%20Group%20on%20Credit%20Histories%20from%20DOF%20web%20site.pdf>

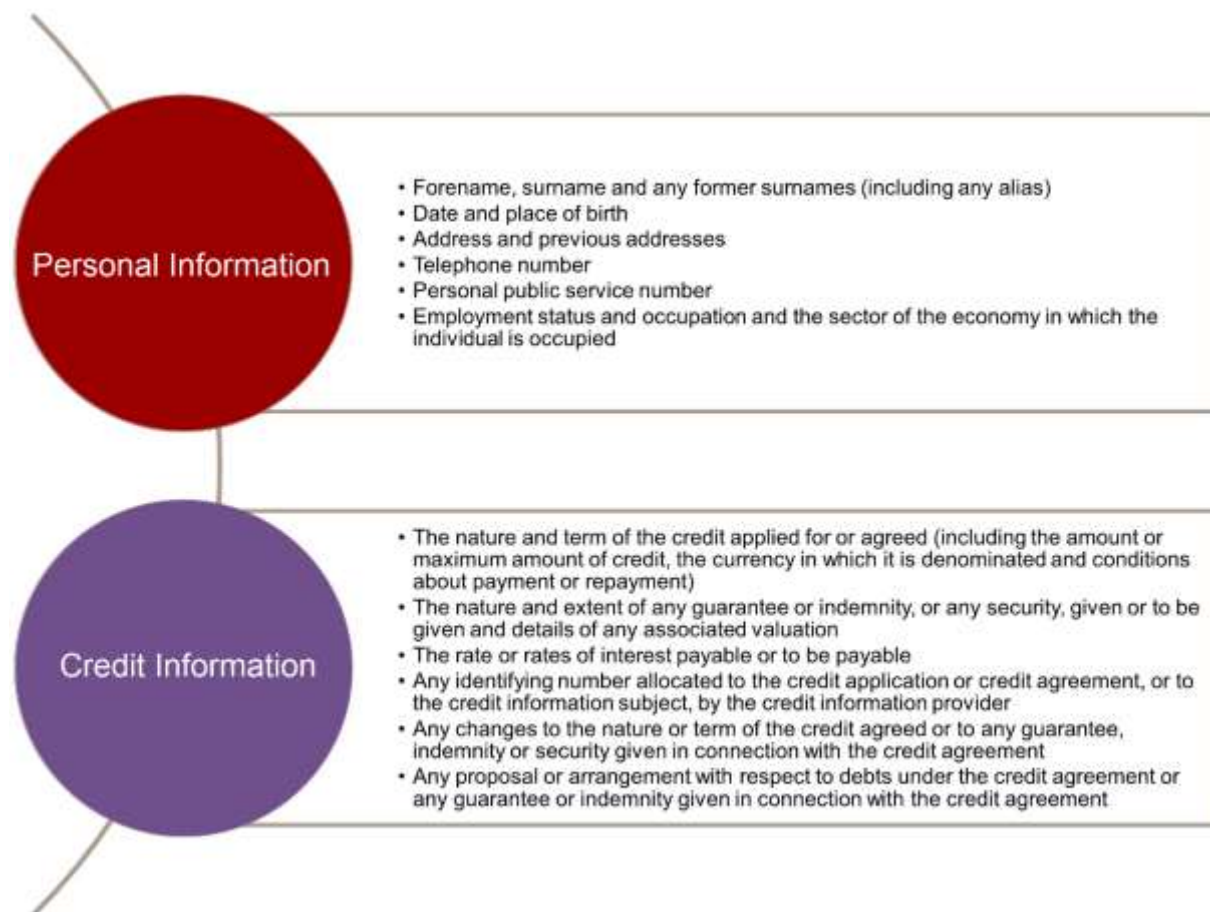
2.8 PRIVACY PRINCIPLE: PROPORTIONALITY

2.8.1 Situation

Decisions about obtaining, processing, disseminating and retaining personal and credit information relating to individuals must consider a proportionate approach within the following parameters:

- The sensitivity of this information to the individual, and
- The corresponding severity of the privacy impact on the individuals when this information is obtained and processed.

The Credit Reporting Act permits the CBI to collect data relating to CISs, however the CBI should consider whether the blanket collection of each data item is proportional to its mandated aim. The Credit Reporting Act 2013 allows the collection of the following personal information¹² relating to CISs and the following credit information¹³ relating to a credit application or credit agreement made by a CIS or a credit agreement in connection with which a CIS is a guarantor.



¹² Section 6, Credit Reporting Act 2013

¹³ Section 7, Credit Reporting Act 2013

2.8.2 Findings

Risk	Impact	Recommendation
<p>2.8.2.1 Fraud</p> <p>There is a risk that the State could be defrauded through the unauthorised disclosure and use of a PPSN to claim social welfare benefits or tax credits they are not entitled to.</p>	<p>There are known instances where individuals have used another person's PPSN to fraudulently claim social welfare benefits or tax credits in another person's name. For either of these frauds to be successful the legitimate owner of the PPSN cannot also be claiming the same benefits or credits.</p> <p>Given this, it is much more likely that people committing a fraud will use the inactive PPSN number of an individual who is not residing in Ireland (there are in excess of 7m PPSNs for a country of 4.6m people).</p> <ul style="list-style-type: none"> In addition, the Department of Social Protection is in the process of rolling out physical public services cards to all welfare claimants. Access to social welfare services will be reliant on each claimant having a public services card which includes photo identification, so access to a PPSN will no longer be sufficient on its own. 	<p>CBI should ensure that PPSN has appropriate security controls over and above the standard controls for personal data, i.e. following Revenue guidance for the use of PPSN and use of file encryption for transmission of submission data over a public network.</p>
<p>2.8.2.2 Snooping</p> <p>There is a risk that the PPSN could be used by private investigators or others for investigations into a CIS.</p> <p>The risk exists that the PPSN could be sourced from a CIP or the CCR directly</p>	<p>Through pretending to be the target individual and using the PPSN with other personal data, an individual may be successful in obtaining information on the target individual from the Department of Social Protection.</p>	<p>CBI should ensure that PPSN has appropriate security controls over and above the standard controls for personal data, i.e. following Revenue guidance for the use of PPSN</p>
<p>CBI Management Response</p> <p>CBI will require CIPs to apply controls similar to those required by the Revenue Commissioners for the collection and storage of PPSN – namely:</p> <p>PPSN may be stored at customer level. [REDACTED]</p> <p>The PPSN should not be shown as part of the customer's standard data. [REDACTED]</p>		

Risk	Impact	Recommendation
<p>In addition, CCR Guidance documentation will highlight the sensitivity of the PPSN and the need for CIPs to keep it safe and secure.</p>		
<p>Within the CCR, access to personal data fields including PPSN will be confined</p>		

2.9 PRIVACY PRINCIPLE: SUBSIDIARITY OF DATA PROCESSING

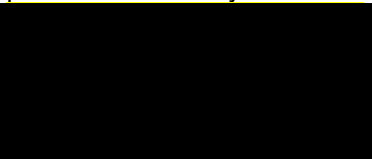

2.9.1 Situation

Subsidiarity of data processing is concerned with minimising the processing of the data at each stage of the process – in other words “*Can the stated aims be achieved using less data?*”

Submission: Each month a full file of personal and facility data relating to CISs with credit agreements will be submitted to the CCR from each CIP

CIP Enquiry: On each enquiry to the CCR, a CIP will submit relevant personal and facility data to identify a CIS and match to any existing records on the CCR.

2.9.2 Findings

Risk	Impact	Recommendation
2.9.2.1 Unnecessary Over-Transmission of Data Each month the full submission of all personal data from CIPs to CCR occurs. This submission file, contains both personal and facility data. 	The transmission of the full Submission data set (e.g. including gender and PPSN) each month represents an overuse of the identifier data contained within the data set.	CBI should consider revising the data submitted to the minimum amount of data required at each point in the cycle.
CBI Management Response In CCR guidance documentation, CBI will set out that the standard approach to monthly reporting of personal data will be:  Target Date for Implementation: From commencement of data submissions [30 June 2017] Person Responsible: CCR Project manager		

2.10 PRIVACY PRINCIPLE: RESPONSIBILITY

2.10.1 Situation

Data Controllers

CIPs: Each CIP is a designated data controller for data stored or processed on its own source systems. This includes the transmission of any source data to the CCR up to when data is received by the CCR.

CBI: The CBI is the designated data controller with responsibility for the operation of the CCR and the data contained within it. The CBI becomes data controller for all credit and personal information contained within the CCR when the data file is accepted for processing into the CCR.

Data Processor

CRIF: The third party CRIF Ireland Limited, in its role in designing, developing and operating the CCR solution, is a data processor and processes all credit and personal information stored on the CCR on behalf of the CBI. The Credit Reporting Act makes the CBI accountable for the establishment and

operation of the CCR and the Bank is ultimately responsible for the activities of its data processor, CRIF Ireland Limited.

2.10.2 Findings

There is clarity and acceptance by both the CIPs and the CBI that they will act as separate data controllers to fulfil the CCR objectives.

Our engagement scope did not include reviewing the controls CIPs are putting in place to mitigate privacy risks. However, our work did establish that the CBI fully accepts the obligations on it as a data controller. Examples of this include completing this PIA, undertaking additional technical security reviews and implementing control processes such as those used to verify the identity of a CIS who requests their credit report.

CBI Management Response

None required

2.11 PRIVACY PRINCIPLE: LIMITATION OF DATA COLLECTION

2.11.1 Situation

The Credit Reporting Act, 2013 sets out the data that may be collected and stored on the CCR. In addition, the Office of the Data Protection Commissioner was involved in consultations on the legislation, and must be consulted on regulations specifying changes to the data which can be collected.

A data model detailing the maximum set of data to be collected as part of Phase I of the CCR Project is in the process of being finalised. This data model specifies the data that will be submitted to the CCR each month by the CIPs via the monthly Submission files. This data can be categorised into three general areas:

- [REDACTED] Data that is required by the CCR for the successful identification and matching of CISs.
- **Credit** Data that relates to the performance of credit agreements held by CISs over a period
- **Statistical** Data that is required by the CBI for the generation of statistics

The CCR will process the data model which contains personal data and facility data relating to individuals including:

- Loan types / mortgage products purchased by the CIS
- Interest rates being paid to CIP
- Status of loans (i.e. the performance of a loan)
- Restructured flag (i.e. Indication of a CIS in financial distress)
- Credit limit
- Outstanding amounts and payments due

- Amount past due (e.g. cumulative amount of missed payments)
- Days past due (the number of days past due as at the reporting date to the CCR)

This entire data model was reviewed as part of the PIA and classified into four categories which have been defined specifically within the context of the CCR and the Credit Reporting Act (2013). These categories take into consideration the sensitivity of the data being collected to the individuals and are broader than the categories of data defined under the Data Protection legislation (See section 1.1.4 for more detail):

- Non-personal data
- Personal data – Normal
- Personal data – Identifiers
- Personal data – Facility

2.11.2 Findings

The Credit Reporting Act, 2013 sets out the data that may be collected and stored on the CCR. In addition, the Data Protection Commissioner must be consulted on regulations specifying changes to the data which can be collected.

CBI Management Response

The CCR data set has been reviewed with a number of stakeholders and as a consequence the following fields will be removed from the final specification.

Personal information

- Mothers maiden name
- Place of birth

Credit information

- Number of times a credit card is used in a month

Target Date for Implementation: Complete

Person Responsible: CCR Project manager

2.12 PRIVACY PRINCIPLE: PURPOSE LIMITATION / LIMITATION OF USE OF PERSONAL DATA

2.12.1 Situation

The Credit Reporting Act specifies the explicit purposes for which the data collected can be used.

CIPs

- Verifying information provided in or in connection with a credit application;

- Evaluating any risk arising from the affording or extending of credit to, or the taking of a guarantee or indemnity from, a credit information subject;
- Evaluating any risk arising from any changes to the nature or term of a credit agreement, or to a guarantee or indemnity given in connection with a credit
- Monitoring any failure to comply with any obligation under a credit agreement or a guarantee or indemnity given in connection with a credit agreement that has not been corrected;
- Evaluating whether to make any proposal or arrangement with respect to the debts of a credit information subject in circumstances in which a credit information subject has made a request for such an evaluation to be made;
- Analysing the nature of the credit information provider's portfolio of credit agreements.

CBI / CCR

- *CBI may use any information held on the CCR in the performance of any of its functions.*
- Currently, the CBI anticipates the uses of the CCR data as follows:
 - CRIF, on behalf of the CBI, will operate the CCR and provide credit reports to CIPs and CISs on enquiry;
 - Granular credit data in anonymised form will be made available to the CBI for analysis in support of its other functions – statistics, prudential supervision, consumer protection, financial stability (note this will be a CCR Project Phase 2 deliverable)

The following user groups will have access to the CCR:

- CCR operators and administrators;
- CIP users for credit application and monitoring enquiries (where the CIS breaches terms and conditions or seeks to restructure loans etc.);
- Access by other third parties [REDACTED] will not be permitted unless there is a legal requirement;
- The system will not be directly accessible by CISs.

CIPs will have access to the CCR to make enquiries for CISs who make an application for credit. CIPs will have access via two methods:

- Web interface
- Application to application interface

2.12.2 Findings

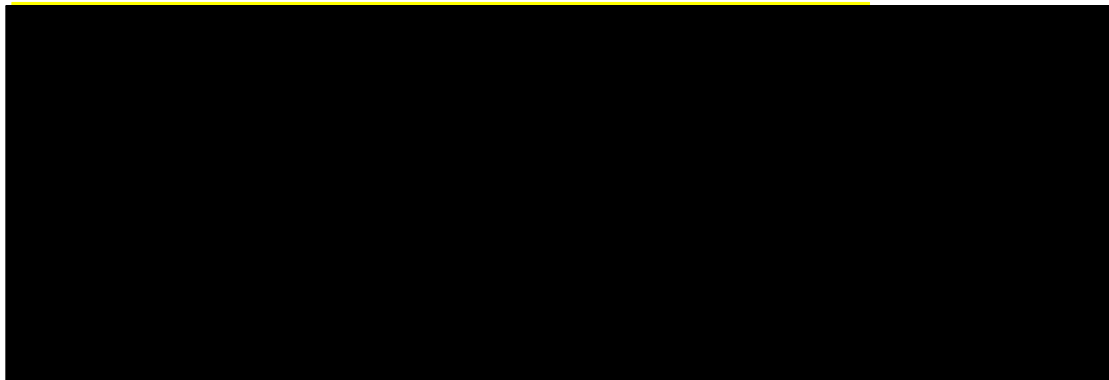
Risk	Impact	Recommendation
2.12.2.1 Unrestricted Use by CBI Section 15 of the Credit Reporting Act appears to grant CBI the legal right to use the information stored in the CCR	Where new or unlimited uses for the data are implemented, there is effectively an	Clarify if the CBI has the right to extend its use of CCR data without the

Risk	Impact	Recommendation
for any of its functions. This creates the risk that CBI uses the data for purposes other than those intended.	obligatory compulsion on CISOs to accept the processing of their data. This is not compatible with the right to a defined and limited use of personal data according to the generally accepted privacy principles.	requirement for additional legislation. If additional legislation is not required to extend the use of data, define a policy and governance to control such changes and manage the associated privacy risks.

CBI Management Response

The Credit Reporting Act 2013 provides a gateway which allows the CBI to access the CCR if it has a statutory purpose for doing so.

The CBI will set out a written [REDACTED] Policy on the use of CCR data within the CBI,



Target Date for Implementation: From commencement of data submissions [30 June 2017]

Person Responsible: CCR Project Manager to prepare a policy statement for approval at Director level.

2.12.2.2 Opportunity for Profiling of Individuals by CIPs If the CCR mandates CIPs capture PPSN, this will result in PPSN being captured on all borrowers (€500 and over) in the state. A CIP could then use the PPSN to profile individual CISOs within an institution using the PPSN as a unique identifier.	If CISOs were mandated to provide their PPSN to secure credit and the PPSN was subsequently used to profile the individual this would constitute using the PPSN for a purpose other than what it was provided for. As such this would be a breach of the individual's privacy. Profiling of CISOs represents a significant impact to the privacy of the individuals as it would be a breach of the privacy	Ensure that all parties with access to the PPSN are aware of the limitations of use of the PPSN as per the legislation.
---	---	---

Risk	Impact	Recommendation
<p>Not all CIPs have solutions in place to provide a single customer view which would allow profiling of individuals to take place. Where this is the case, the use of the PPSN in the CCR would provide an identifier that would be very useful to CIPs in building profiling solutions.</p>	<p>principle of only using personal data for the purposes it was provided for and the CISs would have no control over the level or extent of profiling that could be achieved. However, it is unlikely that a regulated entity such as a CIP would knowingly design a technology solution that breaks the law.</p>	
<p>CBI Management Response</p> <p>Agreed Actions</p> <p>CBI will highlight in its instructions and guidance to CIPs the legislative restrictions on use of CCR information and PPSN in particular for credit assessment purposes only and draw attention to the consequences of breach of these requirements.</p> <p>Target Date for Implementation: Prior to commencement of CCR data collection [30 June 2017] and on an on-going basis thereafter</p> <p>Person Responsible: CCR Project Manager</p>		
<p>2.12.2.3 Increased Profiling of Individuals by Government Agencies or State Bodies</p> <p>Where the PPSN is used in the CCR database it could potentially be used to profile individuals' interactions and behaviour with other agencies or bodies, e.g. Revenue Commissioners, Social Welfare etc.</p> <p>However, at time of writing, we understand that this risk is theoretical only, i.e. we understand that there is no legislation in place that would allow sharing of the CCR data with other state bodies or agencies</p>	<p>There may be benefits to the state in being able to profile individuals' interactions and payments across multiple state bodies or agencies and the CCR, e.g. detecting a fraud. This type of profiling would have the benefit to society of detecting crime. However, it would also be a breach of the privacy principle of only using personal data for the purposes it was provided.</p> <p>Profiling of CISs represents a breach of the privacy principle of only using personal data for the purposes it was provided for.</p>	<p>Ensure that all parties with access to the PPSN are aware of the limitations of use of the PPSN as per the legislation.</p>
<p>CBI Management Response</p> <p>Agreed Actions</p> <p>Any request from Government Agencies or State Bodies for access to CCR data will be reviewed to ensure that it is in accordance with the guidance issued by the Office of the Data Protection Commissioner in respect of Data Sharing in the Public Sector which would include having a clear legislative basis and purpose and that the data provided is consistent with stated purpose.</p>		

Risk	Impact	Recommendation
<p>Target Date for Implementation: As the need arises</p> <p>Person Responsible: CCR Head of Function</p>		
<p>2.12.2.4 CIP Enquiry when Credit Decision is Already Made</p> <p>As per the Credit Reporting Act, every application for credit over €2000 requires an enquiry to the CCR. Where the CIS will not be granted credit under the CIPs credit policy there is still an obligation on the CIP to enquire to the CCR.</p> <p>Such an enquiry, when a CIP decision not to grant credit is already made is not consistent with using the data for the purpose it was provided.</p>	<p>The CIS application data may be sent by the CIP to the CCR for a purpose other than what it was provided for i.e. securing credit. It would instead be sent to comply with the legislative obligations placed on the CIP by the Credit Reporting Act.</p> <p>A CIS may find its data being recorded on the CCR and a Credit Report provided to a CIP when there is no credit decision to be made.</p>	<p>The CBI should ensure that regulations adequately provide for situations such as this, and that a legitimate purpose is required for a CIP to make an application enquiry on the CCR.</p>
<p>CBI Management Response</p> <p>Agreed Actions</p> <p>CBI will highlight in its instructions and guidance to CIPs that they are obliged to check the CCR prior to approving credit applications and they need not check the CCR if they have already decided to reject a credit application under internal credit policies.</p> <p>Target Date for Implementation: Prior to commencement of enquiries against the CCR from [31 December 2017]</p> <p>Person Responsible: CCR Project Manager</p>		
<p>2.12.2.5 Quantity of Data Returned</p> <p>The Credit Reports returned from an enquiry to the CCR will include both personal and facility data relating to a CIS. Only the data that is required to confirm the identity of the CIS and present a clear level of indebtedness and repayment behaviour should be returned. For example where the CIS does not provide a phone number to the CIP, the CCR should not provide phone numbers of the CIS to the CIP.</p>	<p>All available personal data within the CCR database will be shared with all CIPs on enquiry. Consequently, CIPs may gain access to personal data which the CIS has chosen not to disclose and was not requested by the CIP to make a credit decision.</p>	<p>Responses to credit enquiries should include only personal data – normal (as per section 1.1.4) which the CIP provided in its enquiry, e.g. the credit reports should not include telephone numbers that the CIS has not provided to the CIP.</p>
<p>CBI Management Response</p> <p>Agreed Actions</p>		

Risk	Impact	Recommendation
<p>The content of the CIP credit report has been reviewed in the light of this finding and modifications have been made to present only information relevant to a credit decision. Examples include:</p> <ul style="list-style-type: none">- Telephone numbers have been removed- Credit performance history on any credit agreement has been confined to the most recent 24 months. <p>Target Date for Implementation: Prior to commencement of publishing CIP credit Reports in January 2018</p> <p>Person Responsible: CCR Project manager</p>		

2.13 PRIVACY PRINCIPLE: DATA QUALITY

2.13.1 Situation

The accuracy and quality of data is the responsibility of the CIPs who will provide the data to the CCR [REDACTED] However, the CCR will perform routine and automated data quality checks [REDACTED]

Submission:

- The CCR will assess all data submitted by the CIPs using a series of pre-processing validation checks before the data is uploaded to the CCR database. These checks include:
 - File structure, type of records and number of fields in a record
- Following loading of the file into a staging area of the CCR database, the following validation steps are performed:
 - *Check Process on Subject*: checks that all mandatory data subject fields required for matching purposes are present and cross checks them to verify consistency between the information provided.
 - *Check Process on Contracts*: checks all mandatory credit contract fields required for matching purposes are present and cross checks them to verify consistency between the information provided.
 - [REDACTED] The CCR will then send two pairs of error files (one summary and one detailed file of errors relating to contracts and to CIS's) to the CIP detailing the errors for resolution.
 - Where a file is deemed to be suitable for loading, the operator will proceed to load the file [REDACTED]

Enquiry

- Enquiries made by CIPs must include information to identify the relevant CIS being enquired but also the associated credit information relating to a credit application for at least one credit facility.

- Enquiry data quality is processed using a similar process as outlined in Submission above.

2.13.2 Findings

Risk	Impact	Recommendation
<p>2.13.2.1 Speed of Rectification</p> <p>The Credit Reporting legislation is compliant with existing Data Protection law to ensure that an error rectification process is in place and that inaccurate data is updated within a defined period of time of 40 days.</p> <p>However, given financial lending decisions, which impact individuals, will be made based on this information, this may be considered too long a time period.</p>	<p>A CIP may reject an application for credit based on incorrect data. The time taken to resolve this known inaccuracy may cause a CIS undue hardship.</p>	<p>CBI should ensure the lead time to amend inaccurate or poor data held on the CCR is minimised due to the significant impact it could have on the affected CIS.</p>
<p>CBI Management Response</p> <p>Agreed Actions</p> <p>The Credit Reporting Act 2013 sets out the requirements and maximum timelines for consideration of requests for amendment of information on the CCR. The CBI will set out in its instructions and guidance the detailed process steps to be followed by CIPs and CISs seeking amendment of information, emphasising that all necessary information should be furnished as quickly as possible to allow prompt decisions. The CBI will ensure that agreed amendments are processed quickly. In addition CBI will specify a limited set of scenarios where a CIP may request urgent correction of data in advance of normal data file submission.</p> <p>It should also be noted that:</p> <ul style="list-style-type: none"> - pending the outcome of a request for amendment, a credit agreement will be flagged as 'Subject to request for amendment' and this flag will be included in all reports published by the CCR; - A CIS may include an explanatory statement on the CCR which will also be included in any credit reports published by the CCR. - Special procedures will be established to allow a CIP request the CCR to amend information urgently on the CCR rather than wait for submission of amendment <p>Target Date for Implementation: Prior to commencement of collection of data onto the CCR from [30 June 2017]</p> <p>Person Responsible: CCR Project manager</p>		


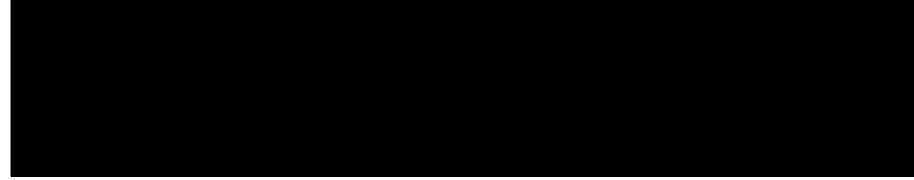
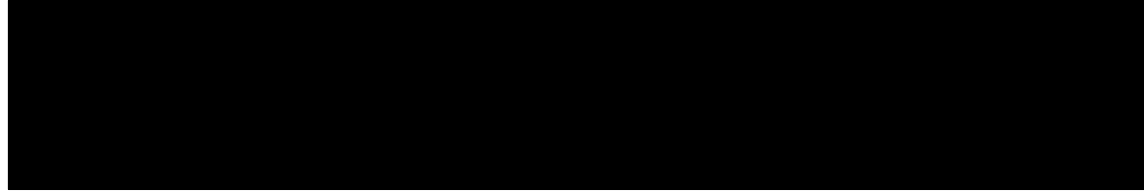
2.14 PRIVACY PRINCIPLE: SECURITY OF DATA

2.14.1 Situation

The CBI has responsibility to ensure the security of all data stored, processed and accessed on the CCR and to prevent against loss of or any form of unlawful processing of the data. [REDACTED]

2.14.2 Findings

Risk	Impact	Recommendation
2.14.2.1 Abuse of access rights to CCR There is a risk that CIP employees could abuse access to the CCR by accessing CCR data for purposes other than evaluating a credit application.	Where a credit report or the credit record of a CIS is accessed when there is no legitimate purpose to do so, there is an invasion of the CISs privacy rights.	Consider the implementation of preventative / detective controls to restrict / monitor CIP staff access to the CCR.
CBI Management Response Agreed Actions The CBI will establish a CCR compliance monitoring function [REDACTED] [REDACTED] Target Date for Implementation: Prior to commencement of enquiries against the CCR from [31 December 2017] and on an on-going basis thereafter Person Responsible: CCR Project Manager		
2.14.2.2 Absence of Submission File Encryption The channel through which the data is submitted to the CCR from the CIP is encrypted. However, the initial design of the submission process does not include file encryption. Given the sensitivity of the submission file, which contains both personal and facility data	[REDACTED]	Industry accepted encryption standards should be considered for the encryption of the submission file. This is in addition to tunnel encryption

Risk	Impact	Recommendation
relating to a CIS, the impact of a security breach to a CIS is potentially very high. As such reliance on tunnel encryption only may not be appropriate.		included in the initial design.
CBI Management Response Agreed Actions   Target Date for Implementation: Prior to commencement of CCR data submissions from [30 June 2017]. Person Responsible: CBI Information Security Manager		
2.14.2.3 Unauthorised Access to the CCR The CCR enquiry service will be available to all internet connected users. As a result, there is a risk of unauthorised access to the CCR via Web access.	Unauthorised access to the enquiry functionality of the CCR could result in the unauthorised or inappropriate dissemination of CIS credit reports.	Apply additional controls that will restrict to enquiries from authorised users within CIPs.
CBI Management Response Agreed Actions A combination of controls will be applied:  Target Date for Implementation: Prior to commencement of enquiries against the CCR from [31 December 2017] and on an on-going basis thereafter Person Responsible: CCR Project Manager		

Risk	Impact	Recommendation
<p>2.14.2.4 Saving Data to Uncontrolled Systems</p> <p>As a CIP employee has the ability to download a PDF copy of a credit report via the web portal, there is a risk of a CIP saving credit reports to uncontrolled systems such as home PCs.</p>	<p>Unauthorised access of CIS credit reports containing identifier and facility data by authorised CIP staff.</p> <p>OR</p> <p>Data breach due to credit reports being stored on insecure home PCs.</p>	<p>Consider strengthening security controls so copies of credit reports can only be downloaded within a controlled CIP environment.</p>
<p>CBI Management Response</p> <p>Agreed Actions</p> <p>CIPs will become data controllers for CCR data received into to their systems or environments in various formats. As such they will have to ensure that the information is processed securely and used only for the purposes specified in the Credit reporting Act 2013.</p> <p>CBI will set out in its instructions and guidance to CIPs the responsibilities associated with accessing and using information sourced from the CCR and require them to provide training to all staff impacted.</p> <div data-bbox="207 1037 1386 1294" style="background-color: black; height: 115px; width: 100%;"></div> <p>Target Date for Implementation: Prior to commencement of enquiries against the CCR from [31 December 2017] and on an on-going basis thereafter</p> <p>Person Responsible: CCR Project Manager</p>		
<p>2.14.2.5 CCR Internal Security</p> <p>The CCR will result in the creation of several new data stores of personal data.</p> <ul style="list-style-type: none"> • CDMS (Customer Data Management System) • CIS emails and backups • Core CCR database <p>There will be a reliance on technical security of the CCR to manage the risk to the security of these data hotspots.</p>	<div data-bbox="609 1529 1118 1646" style="background-color: black; height: 52px; width: 100%;"></div>	<p>CBI should ensure that appropriate security controls are established within the CCR and that regular testing takes place to validate the effectiveness of these controls.</p>

Risk	Impact	Recommendation
<p>CBI Management Response</p> <p>Agreed Actions</p> <div data-bbox="204 412 1378 757" style="background-color: black; height: 154px; width: 100%;"></div> <p>Target Date for Implementation :Before commencement of Submissions 30 June 2017</p> <p>Person Responsible: CCR Head of Function</p>		
<p>2.14.2.6 Management of Data Subject Access Requests</p> <p>There is a risk that an additional personal data hotspot is created within the CBI due to the management of data subject access requests (DSARs) made by a CIS for their data stored both within CBI and the CCR.</p>	<p>Where additional data hotspots are created in the CBI (outside the CCR), data may not be managed in line with the CCR requirements, increasing the risk of a data breach.</p>	<p>CBI should ensure that the DSAR process is adequately considered within the CCR project and necessary controls are implemented.</p>
<p>CBI Management Response</p> <p>Agreed Actions</p> <div data-bbox="204 1400 1378 1440" style="background-color: black; height: 18px; width: 100%;"></div> <div data-bbox="204 1440 1378 1529" style="background-color: black; height: 40px; width: 100%;"></div> <p>Arrangements for storage of and access to CCR personal data within the CBI will be updated to take account of the nature and scale of the personal data involved.</p> <div data-bbox="204 1561 1378 1650" style="background-color: black; height: 40px; width: 100%;"></div> <p>Target Date for Implementation: Prior to commencement of CIP submission of data to the CCR from [30 June 2017]</p> <p>Person Responsible: CBI Data Protection Officer</p>		
<p>2.14.2.7 Sensitive Data Stored by Third Parties</p> <p>CISs may make credit applications to CIPs through third parties. Where this takes</p>	<p>Unauthorised storage of the application data for longer than is required by the third party increases the likelihood that</p>	<p>All data controllers are required to</p>

Risk	Impact	Recommendation
<p>place, there is a risk that the third parties may store or retain the credit application containing CIS personal data, including PPSN, after the application is submitted to the CIP.</p> <p>This risk is increased where the third parties are unregulated entities (e.g. car dealerships) as the CBI does not have a direct or indirect role in regulating these businesses and cannot mandate controls or behaviour.</p>	<p>further use, processing or breach of the CIS data may occur.</p> <p>We note that while this risk exists in the pre-CCR environment, the use of the PPSN in the CCR dataset would increase the potential negative consequences of this risk materialising</p>	<p>comply with the Data Protection Acts.</p> <p>The CIPs are data controllers in their own right and it does not fall to the CBI to prescribe to the CIPs how to comply with the Data Protection Acts.</p> <p>In addition, unregulated data controllers are also required to comply with the Data Protection Acts. In the case of these entities the CBI has no mandate to dictate how this is done.</p> <p>CISs must be aware of their rights under the DP Acts and make decisions on sharing their data in an informed manner. We do not see this as the job of the CBI.</p>
<p>CBI Management Response</p> <p>Agreed Actions</p> <p>CIPs are data controllers for data collected for internal processing and reporting to the CCR. Where agents or intermediaries collect and process data on behalf of CIPs they are subject to influence and instructions from the CIPs.</p> <p>The Credit Reporting Act 2013 imposes obligations on CIPs to notify CISs of their rights and duties under the CRA and of the obligation to report data to the CCR.</p> <p>CBI will set out in its instructions and guidance to CIPs the responsibilities associated with collecting and processing data for submission to the CCR and their obligations to inform CISs of their rights and duties under the CCR.</p> <p>Target Date for Implementation: Prior to commencement of enquiries against the CCR from [31 December 2017] and on an on-going basis thereafter</p> <p>Person Responsible: CCR Project Manager</p>		

2.15 PRIVACY PRINCIPLE: TRANSPARENCY

2.15.1 Situation

Credit and personal data will be collected and submitted to the CCR by the CIPs. Section 23 of the Act¹⁴ mandates that all CIPs must ensure that individuals are made aware of their rights and duties under the Act, in line with existing provisions under the Data Protection Act. Section 24 of the Act mandates that all CIPs shall provide notice on their forms and paperwork relating to qualifying credit applications that the information will be provided to the CBI for the purposes of entry on the CCR.

2.15.2 Findings

Risk	Impact	Recommendation
2.15.2.1 Transparency of Use of Data <p>There is a risk that CISs may not be made aware of all of the purposes their data is being used for or the full breadth of data being sent to the CCR. This is especially true where the uses of the data by the CBI changes over time.</p>	<p>Where the uses of the data are not transparently understood by a CIS, the CIS may not make be adequately informed about submitting their data to a CIP for inclusion on the CCR.</p> <p>In the absence of consent required for the data to be submitted to the CCR, any erosion of the transparency of the uses of the data further impacts on the privacy rights of an individual CIS.</p>	<p>The uses and purposes for collecting CIS data should be fully and transparently communicated to the CIS at the point at which the data is obtained and subsequently where the use of the data changes.</p>
CBI Management Response <p>Agreed Actions</p> <p>The CBI will set out in its instructions and guidance to CIPs the nature of the information to be provided to CISs at the time of making credit applications and more generally.</p> <p>The CBI will publish information for CISs on the role and purpose of the CCR, the nature of the data to be collected and the uses to which it will be put. It will also explain the rights of CISs e.g.:</p> <ul style="list-style-type: none"> - To access a copy of their own credit report - To enter explanatory statements on their credit record - To seek amendment of errors - To register any suspicion of impersonation <p>Target Date for Implementation: Prior to commencement of data submission to the CCR from [30 June 2017]</p> <p>Person Responsible: CCR Project Manager</p>		
2.15.2.2 Notification of Existing Loans Submitted to CCR <p>There is a risk that the CISs will not be adequately or appropriately notified of the</p>	<p>In the absence of consent required for the inclusion of existing loans on the CCR, any erosion of the transparency of</p>	<p>A CIS should be informed what data is being sent to the</p>

¹⁴Credit Reporting Act 2013

Risk	Impact	Recommendation
inclusion of existing loans by their CIPs to the CCR.	the uses of the data further impacts on the privacy rights of an individual CIS.	CCR and the purposes of this data prior to the data being transferred to the CCR.
CBI Management Response Agreed Actions The CBI will set out in its instructions and guidance to CIPs the nature of the information to be provided to CISs whose loans will be reported to the CCR from the data of commencement. The CBI will publish information for CISs on the role and purpose of the CCR, the nature of the data to be collected and the uses to which it will be put. It will also explain the rights of CISs e.g.: <ul style="list-style-type: none"> - To access a copy of their own credit report - To enter explanatory statements on their credit record - To seek amendment of errors - To register any suspicion of impersonation Target Date for Implementation: Prior to commencement of data submission to the CCR from [30 June 2017] Person Responsible: CCR Project Manager		

2.16 PRIVACY PRINCIPLE: RIGHTS OF INDIVIDUALS

2.16.1 Situation

CISs have the right to access, correct, supplement or request deletion of their data held on the CCR and have the right to consent for their data to be processed.

The Credit Reporting Act¹⁵ does not permit a CIS to delete or remove their personal data or to oppose the processing methods; however, it does make provisions for the CIS to access their information held on the CCR (Section 15) and the right to the correction of any incorrect or inaccurate information (Section 9). The maximum periods for which data relating to a CIS may be held are set out in Section 8 of the Credit Reporting Act.

Additionally, any person can be granted access to a CISs information once they have been delegated authority by that CIS (Section 15).

2.16.2 Findings

Risk	Impact	Recommendation
2.16.2.1 Absence of CIS Consent for Data Processing The Credit Reporting Act gives the CBI the legislative power to process data without an individual's consent . While	Consent of the individual is a strong foundation of privacy practices.	Individuals should be asked to explicitly acknowledge the use of their data by

¹⁵ Section 15, Credit Reporting Act 2013

Risk	Impact	Recommendation
an individual could, theoretically, choose not to apply for credit and so avoid sharing their data with the CCR, this is not true for existing loans where the applicant which will be included in the CCR database.	Although the Credit Reporting Act enables processing of personal data without consent, this is a distinct and deliberate departure from standard privacy practices.	the CCR as part of the credit application process.
CBI Management Response Agreed Actions The Credit Reporting Act 2013 sets out that CISs are to be informed at the time of making a credit application of the obligation to report their information to the CCR. The CBI has set out in a regulation the wording of a notice to be provided to CISs by CIPs. However, it is not intended to seek explicit acknowledgement from CISs of the use of their data within the CCR as this could be confused with consent. The information must be reported to the CCR regardless of whether or not a CIS gives explicit acknowledgement of use of the information by the CCR. Target Date for Implementation: Prior to commencement of data submission to the CCR from [30 June 2017] Person Responsible: CCR Project Manager		

2.17 ADDITIONAL ITEMS FOR CONSIDERATION

The point-in-time nature of this PIA occurring within the design phase of the CCR project lifecycle means that there are a number of areas which have not yet been finalised. These should be addressed through the delivery and execution of the detailed project plan.

The PIA has considered these against the privacy principles and identified a number of items which, although they do not currently represent privacy risks, could give rise to significant privacy risks in the future if they are not managed appropriately.

The following items which have implications across multiple privacy principles were identified and it is recommended that consideration is afforded to addressing these items in the delivery of the CCR project plan.

2.17.1 Clear Definition of Roles, Responsibilities and Operational Processes

The roles and responsibilities of all participants and stakeholders within the end-to-end CCR solution are not yet clearly defined or communicated in all cases. This requires the definition of responsibilities throughout the end-to-end CCR processes and across all individual process steps including, for example:

- Data decisions relating to data collected, processed, stored and shared.
- Management and day-to-day operations of the CCR e.g.:

- Data controller role of CBI and appropriate boundaries
 - Data controller role of CIPs and appropriate boundaries
 - Data processor
 - Data consolidation
 - Data submission
 - Data quality management
 - Data breach management
 - Error resolution
 - Issue escalation
- Oversight of outsourced third party activities including transparency of operations, security, CIS support, CIP support, etc.
 - Operational processes, which will impact the privacy of CISs will need to be defined, e.g.:
 - Identity verification and validation of CISs: Credit reports will contain personal and sensitive facility data, therefore the process to validate and verify a CISs identity during the CIS enquiry process is critical.

Relevant Privacy Principles:

- Responsibility

2.17.2 Third Party Outsourcing by CIPs

The PIA learned that a number of CIPs are exploring solutions involving outsourced third party partners which would provide a multi-bureau enquiry and/or data consolidation services or value added services that may impact the privacy of a CIS.

This introduces the possibility that a multi-bureau credit industry could exist in Ireland for the first time, and some CIPs are exploring the option of utilising as many sources of credit information as possible to inform their credit lending decisions. The architecture and data flows associated with this potential solution may introduce additional privacy risks for individuals which have not been considered as part of the scope of this PIA.

Relevant Privacy Principles:

- Responsibility
- Transparency
- Purpose Limitation
- Security

2.17.3 Breach Notification

At the point in time when this PIA was undertaken, the policy and supporting processes for identifying, handling, reporting and mitigating data breaches relating to CCR data had not been determined. There is a dependency on the roles and responsibilities between CBI, CCR and CIPs being defined,

communicated and understood by all relevant stakeholders to ensure breaches are responded to appropriately.

Relevant Privacy Principles:

- Responsibility
- Transparency
- Purpose Limitation
- Security

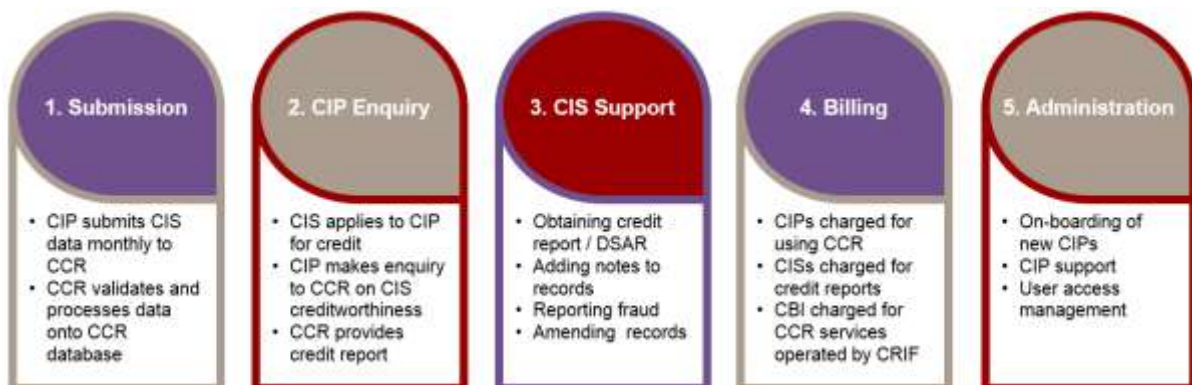
3 DESCRIPTION OF THE CCR SYSTEM, PROCESSES AND DATAFLOWS

3.1 INTRODUCTION TO THE CCR SYSTEM

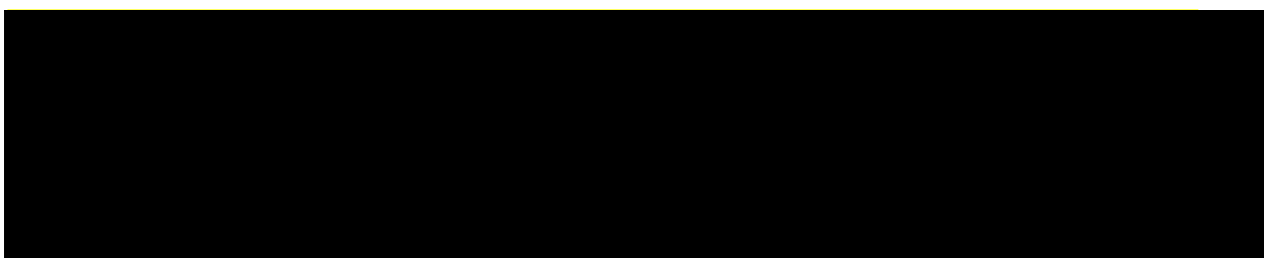


3.1.1 CCR Macro Processes

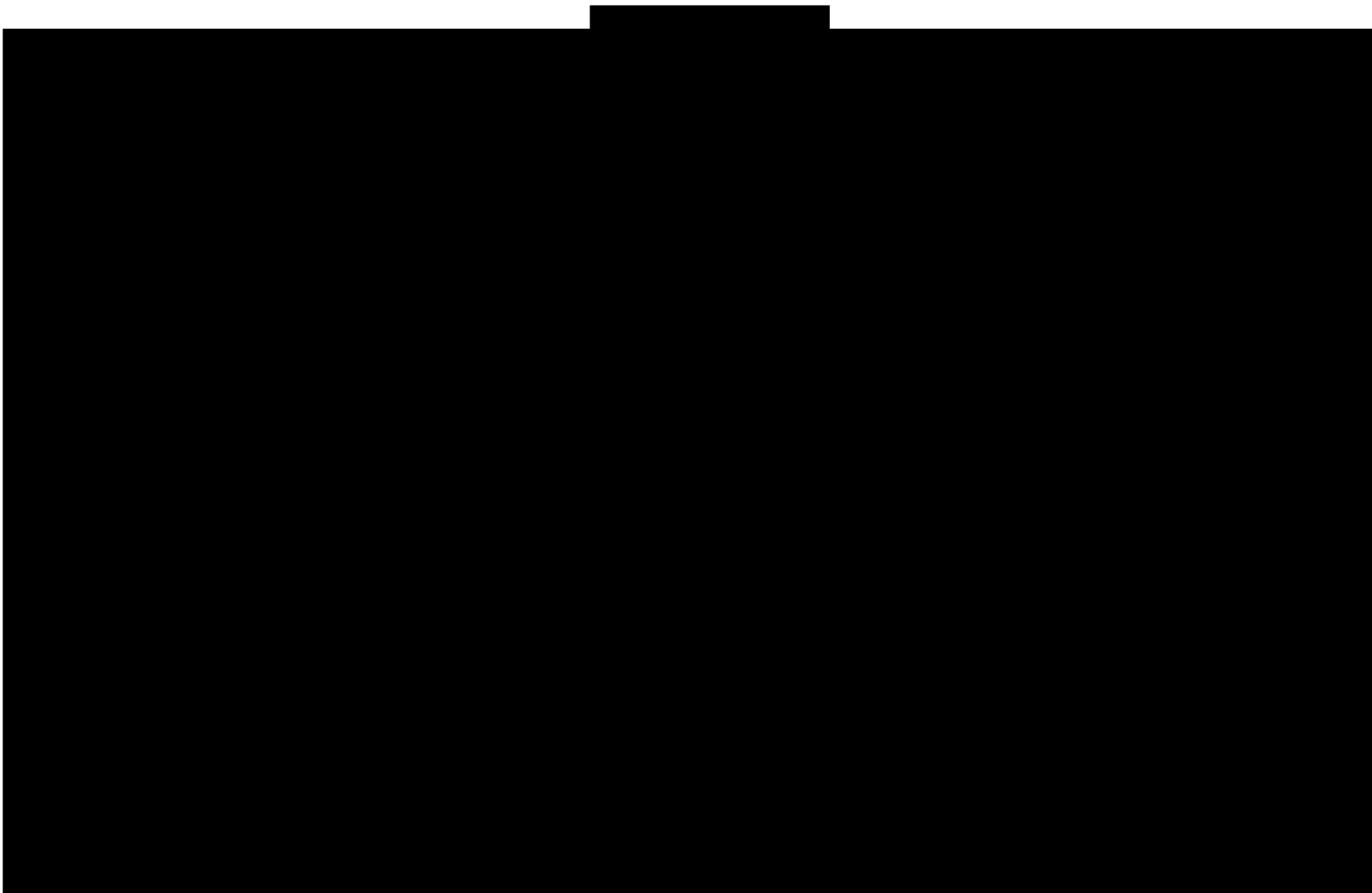
The PIA assessed the following macro-processes that will be introduced to manage the CCR. We prepared detailed data flows to assist the identification of privacy risks and these are outlined in section 3.1.2 below.

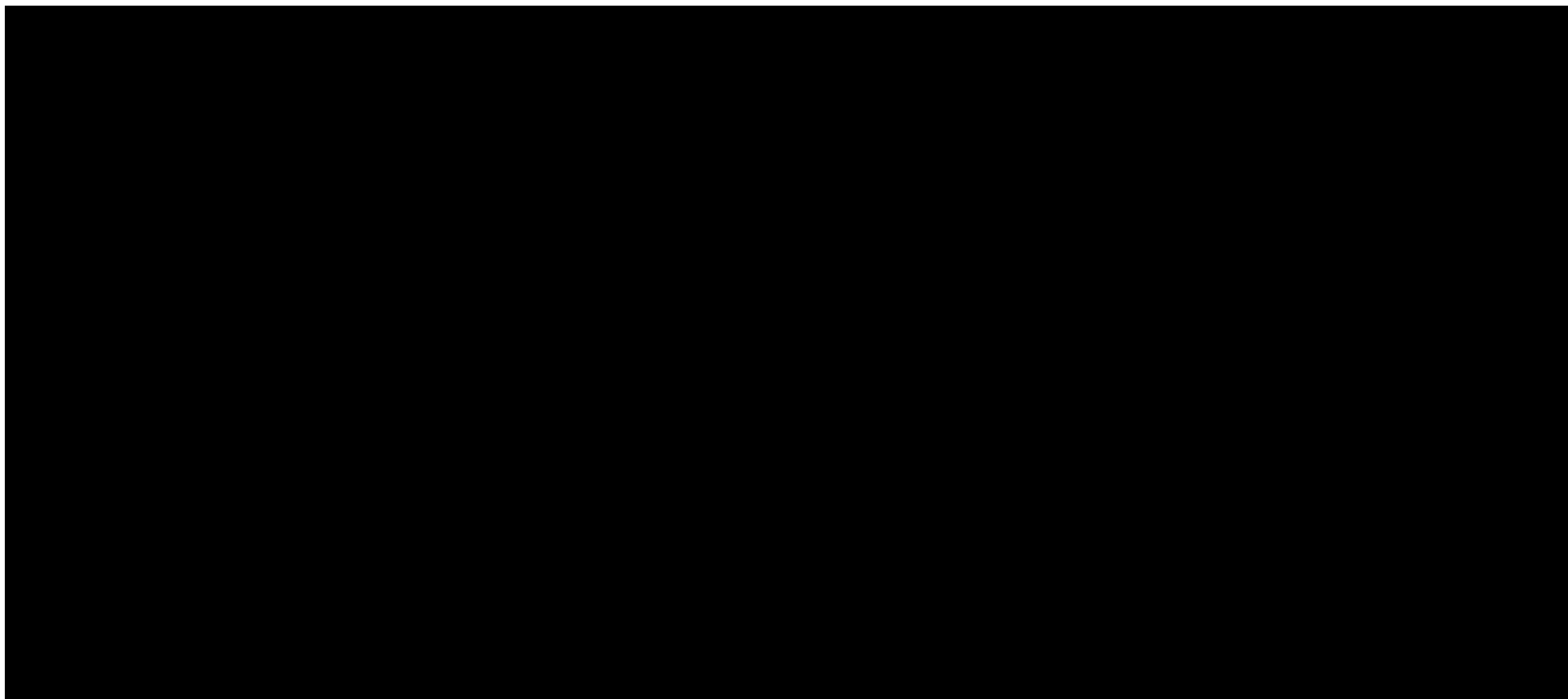


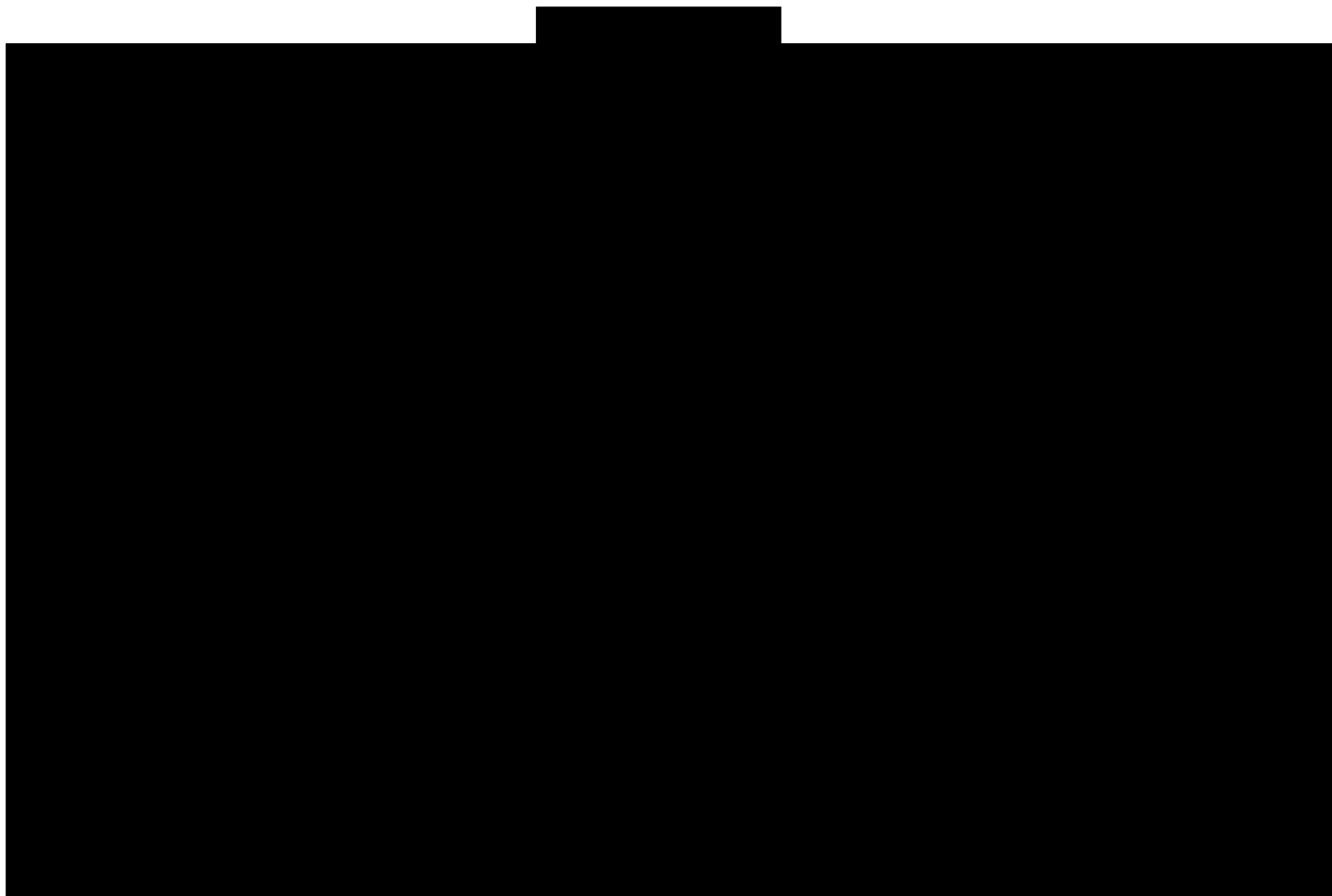
3.1.2 Data Flows

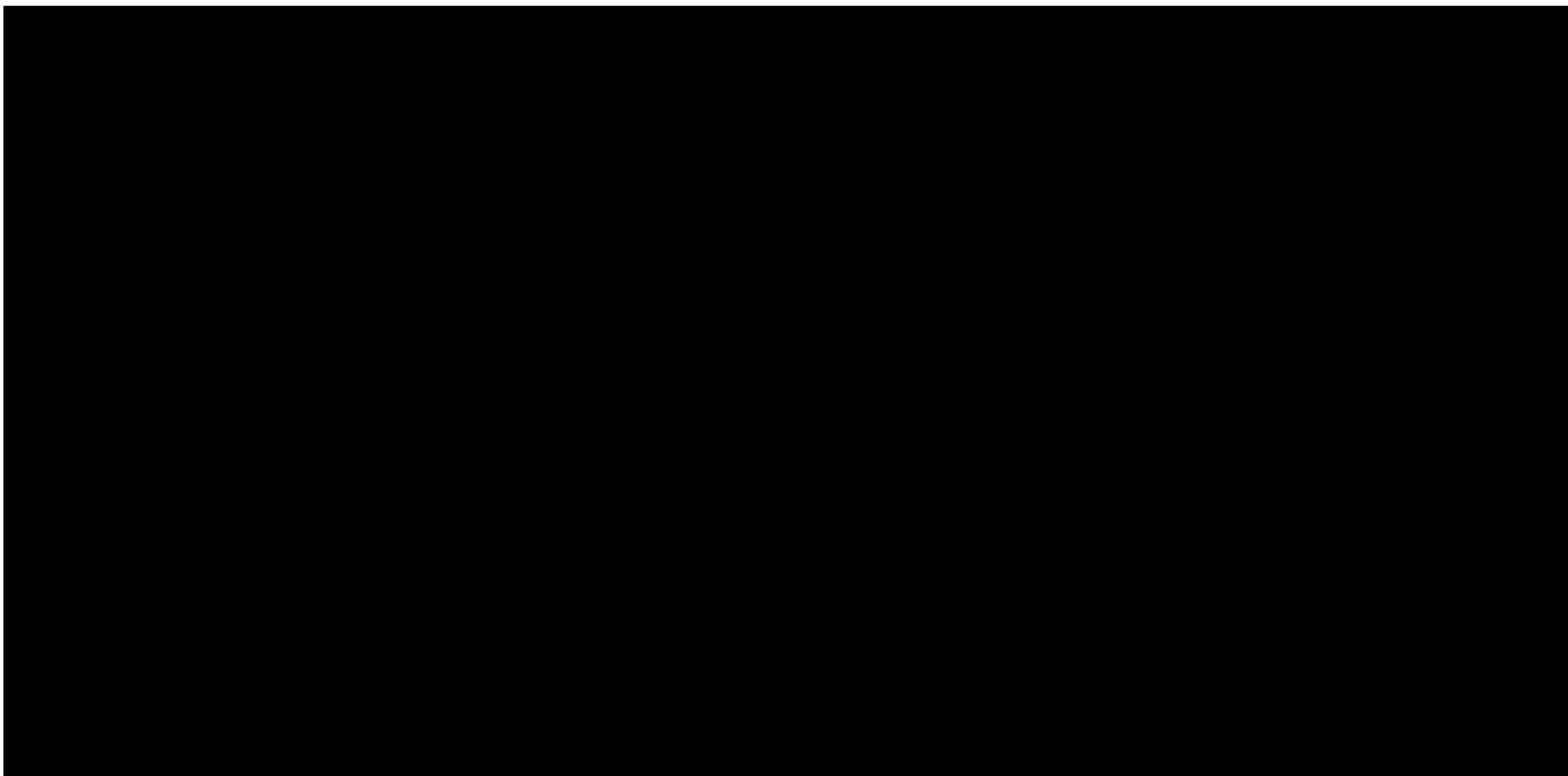


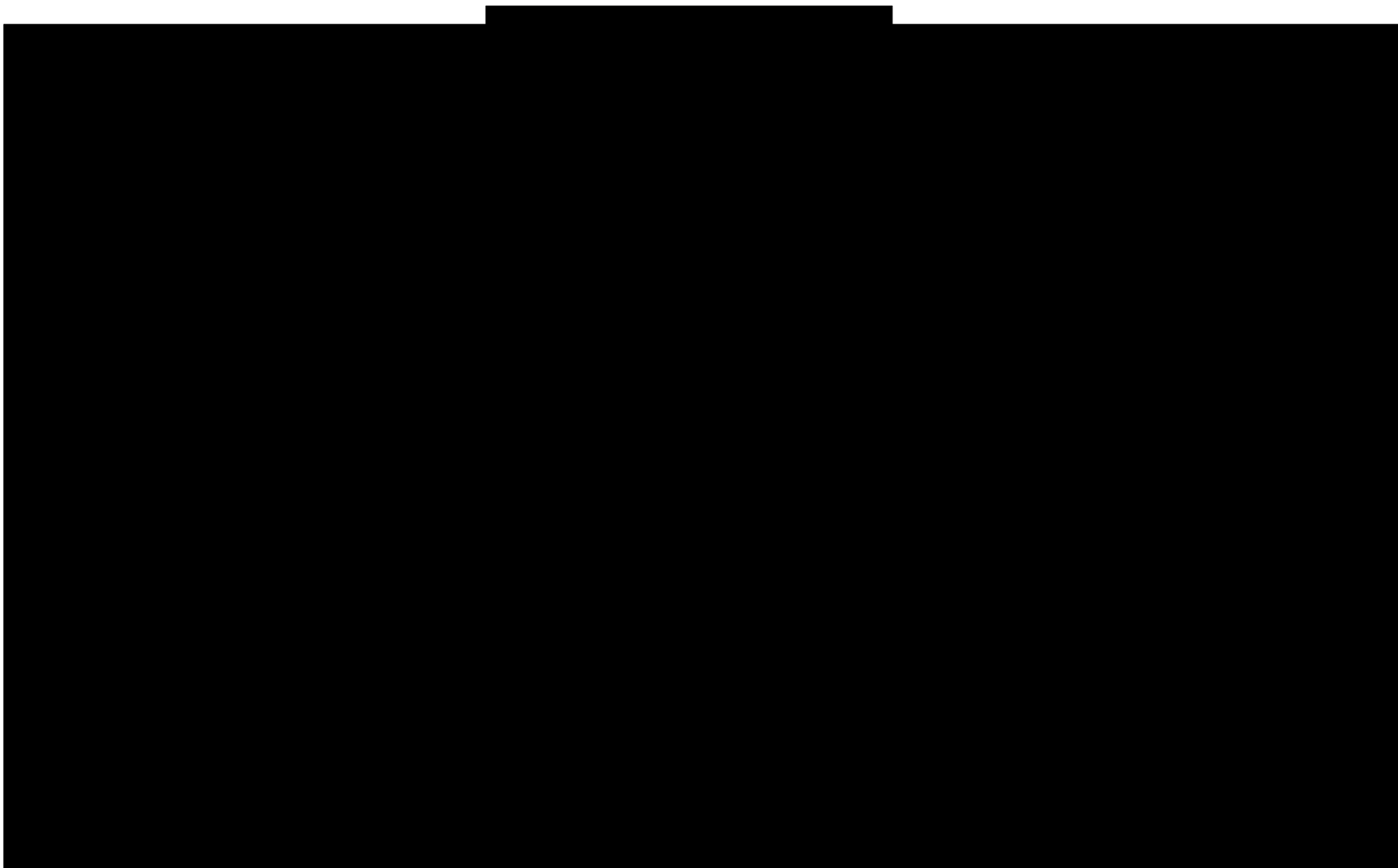


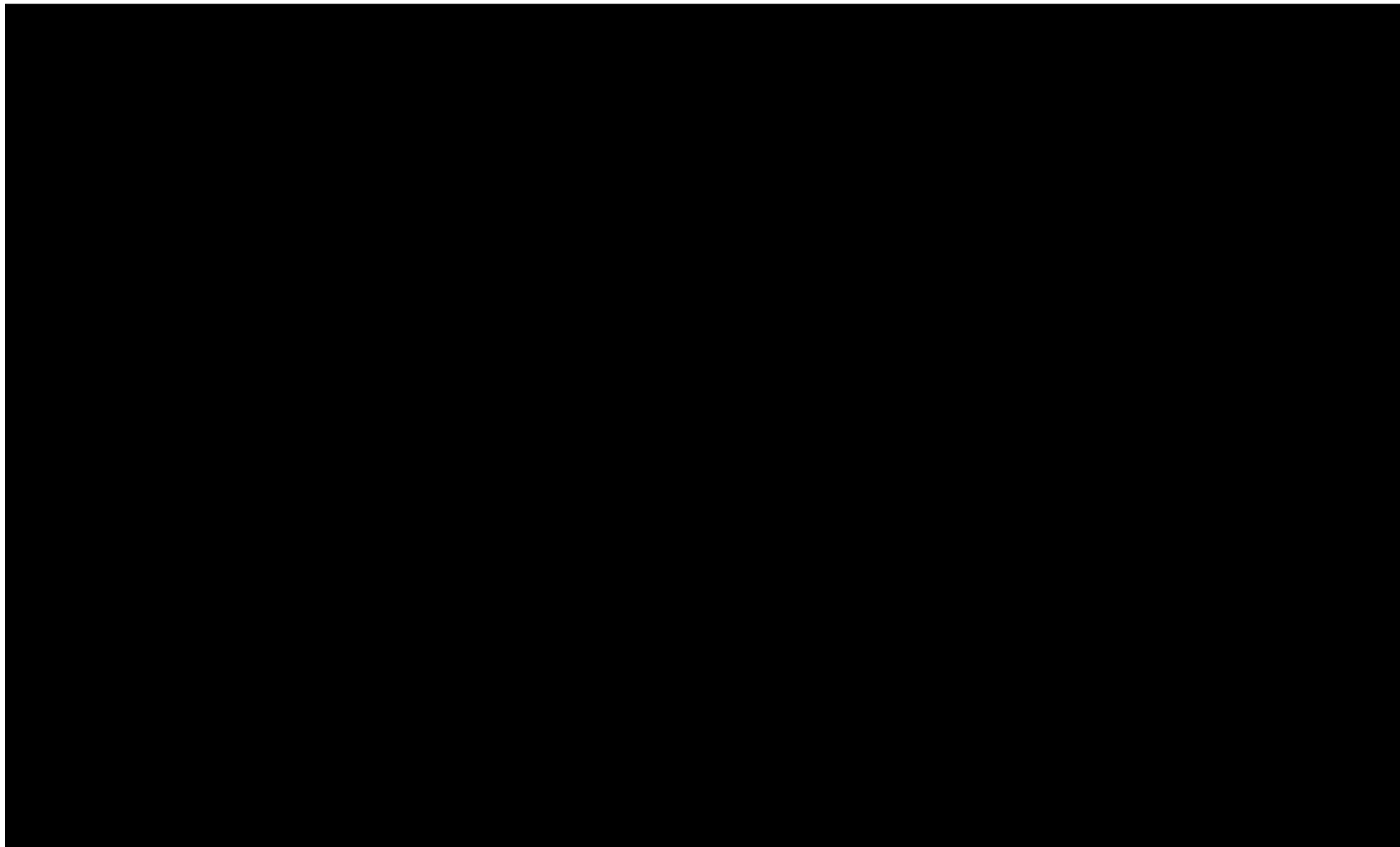


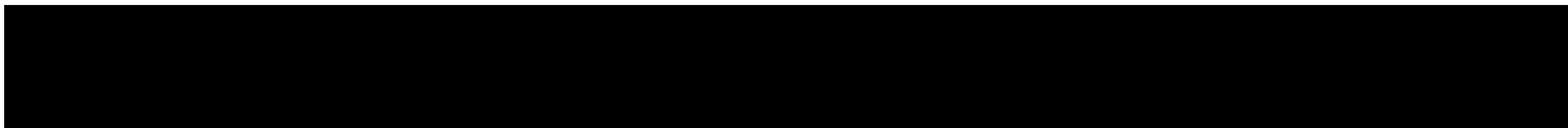


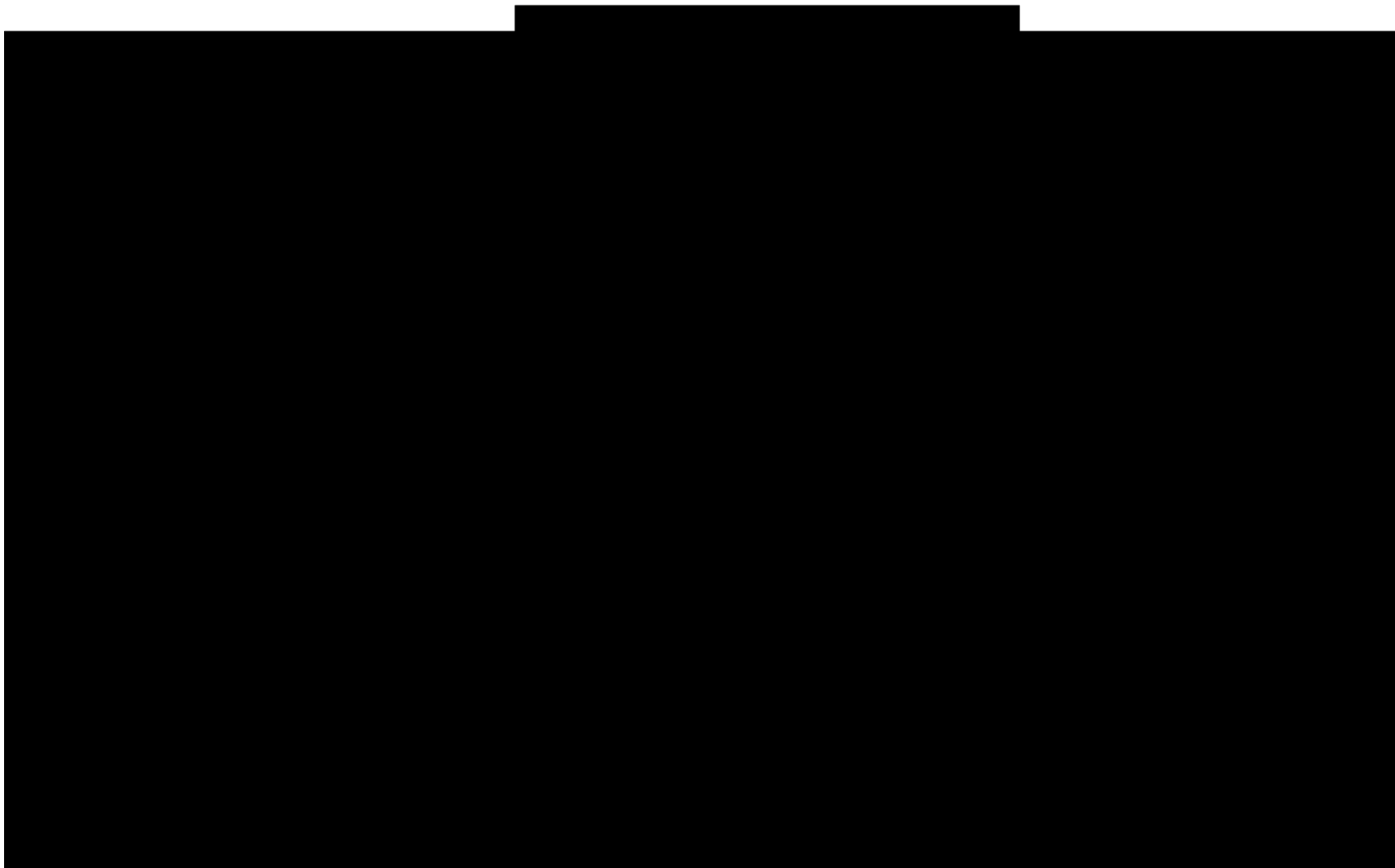


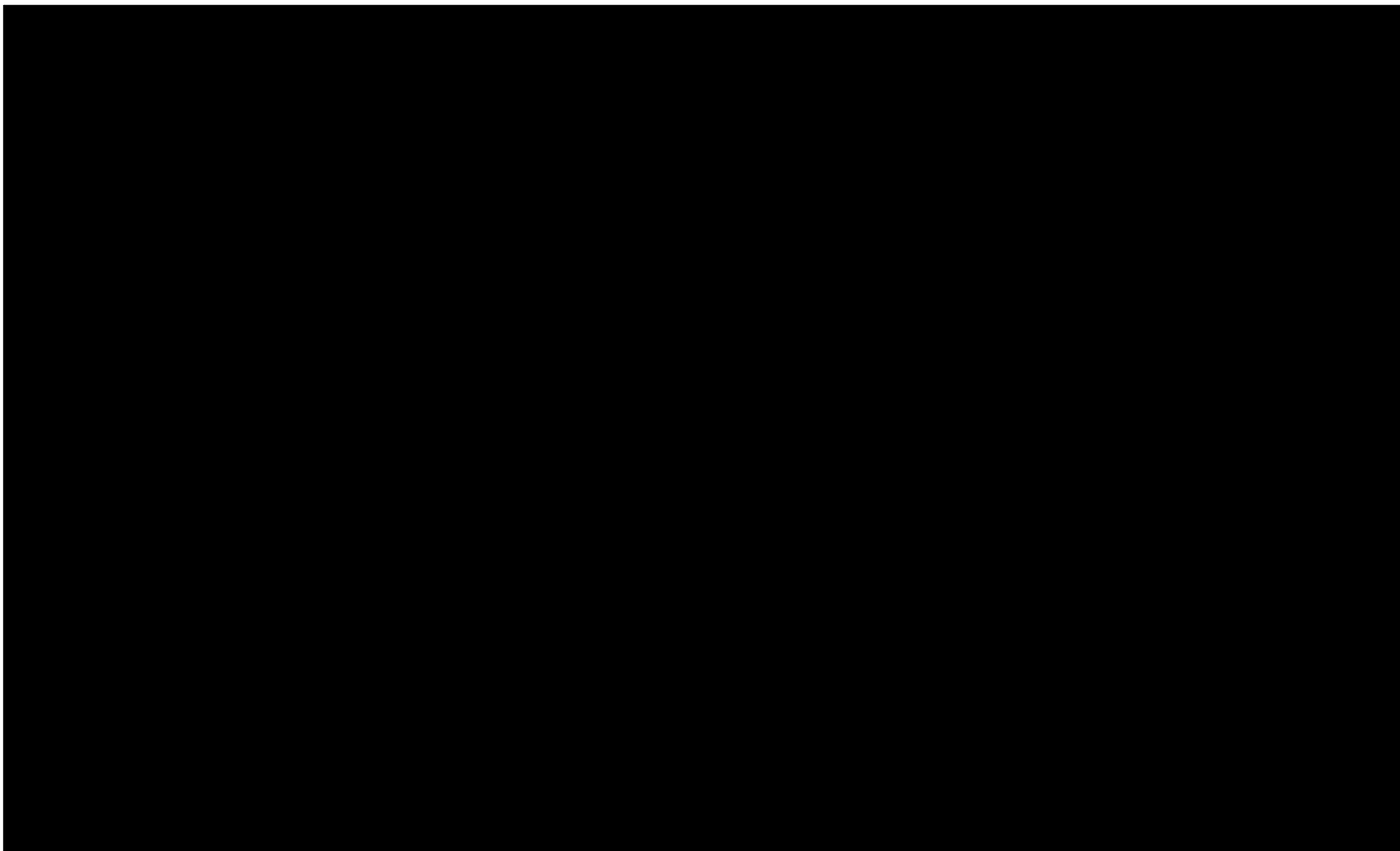


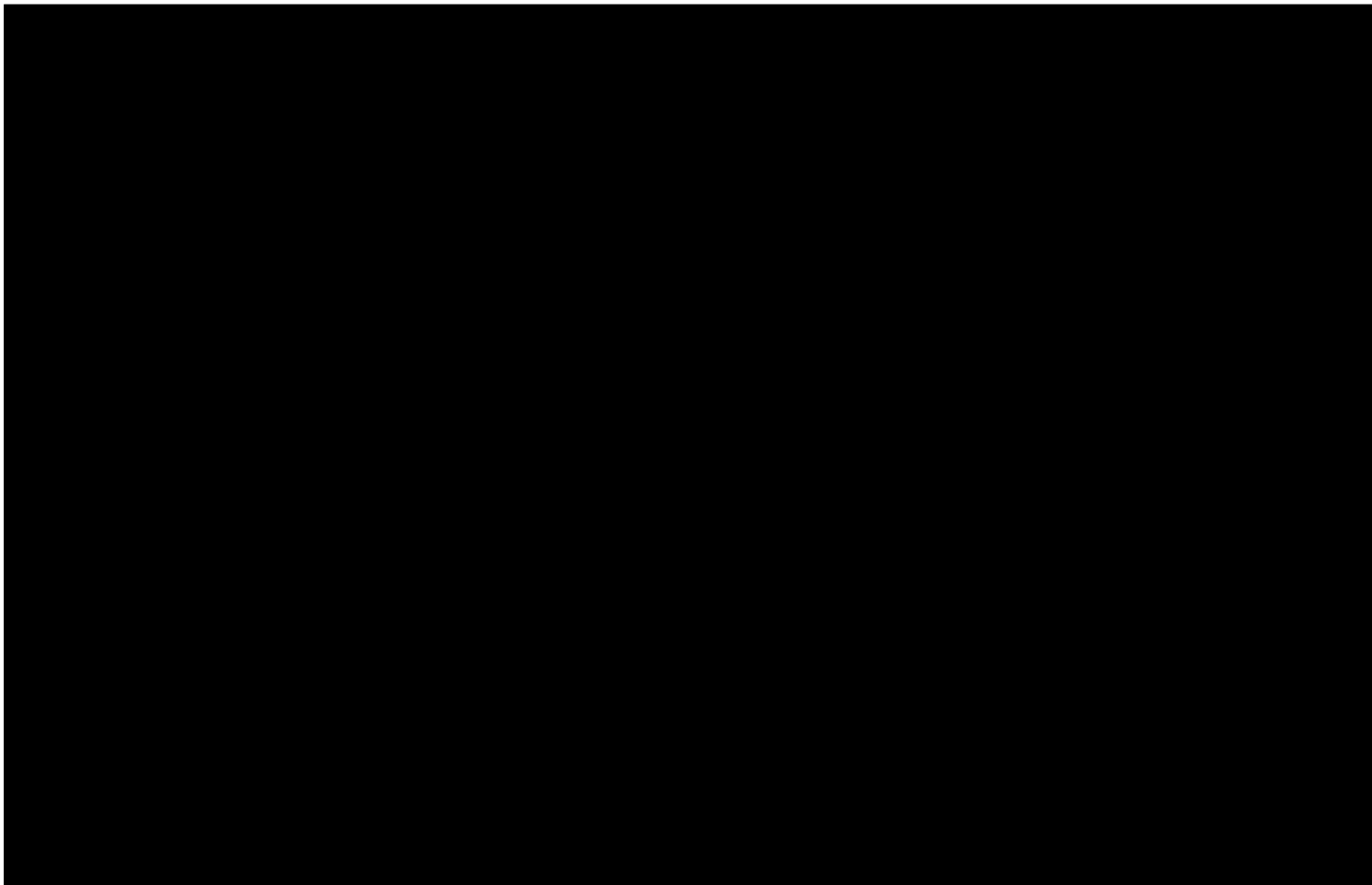


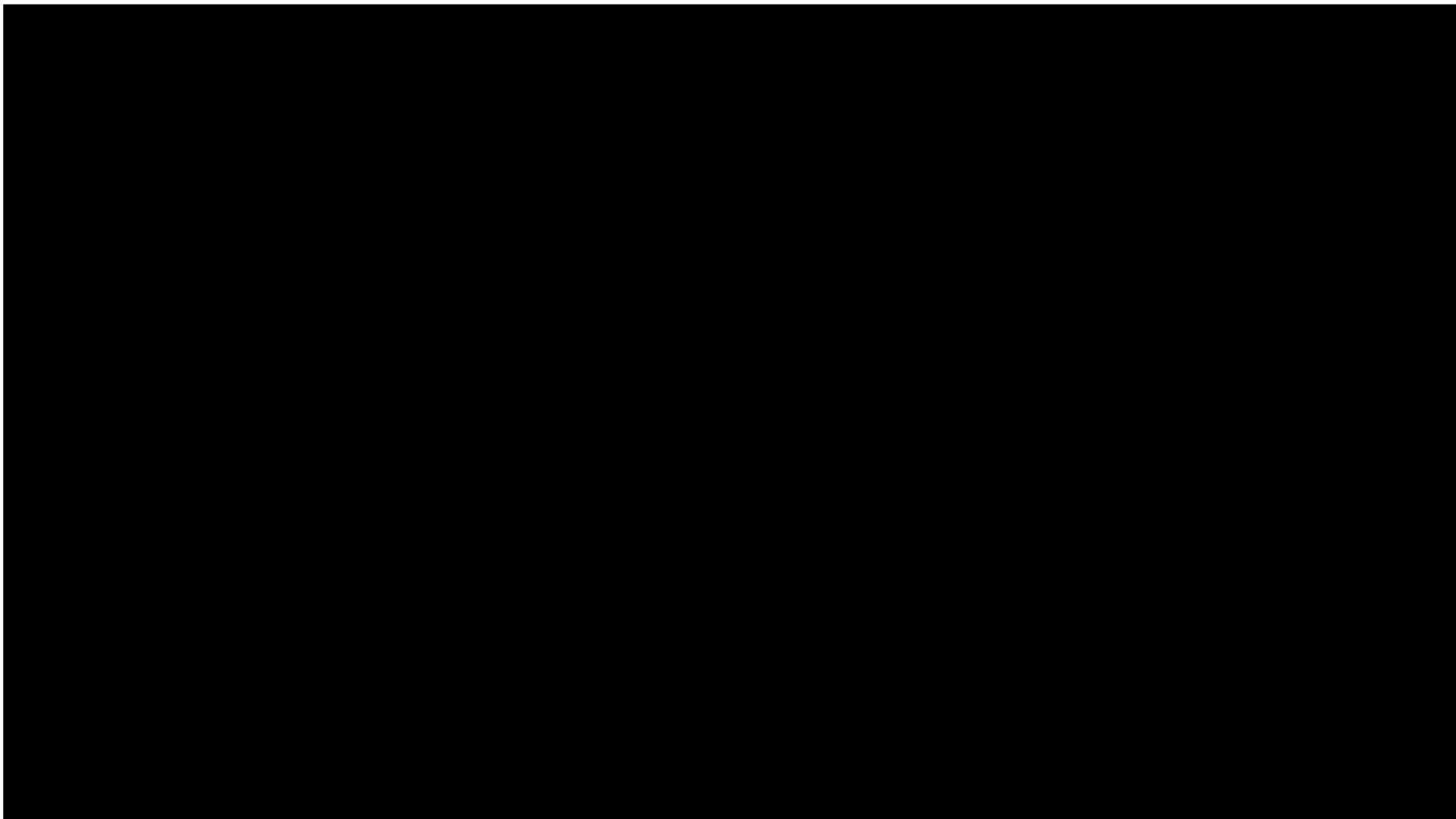


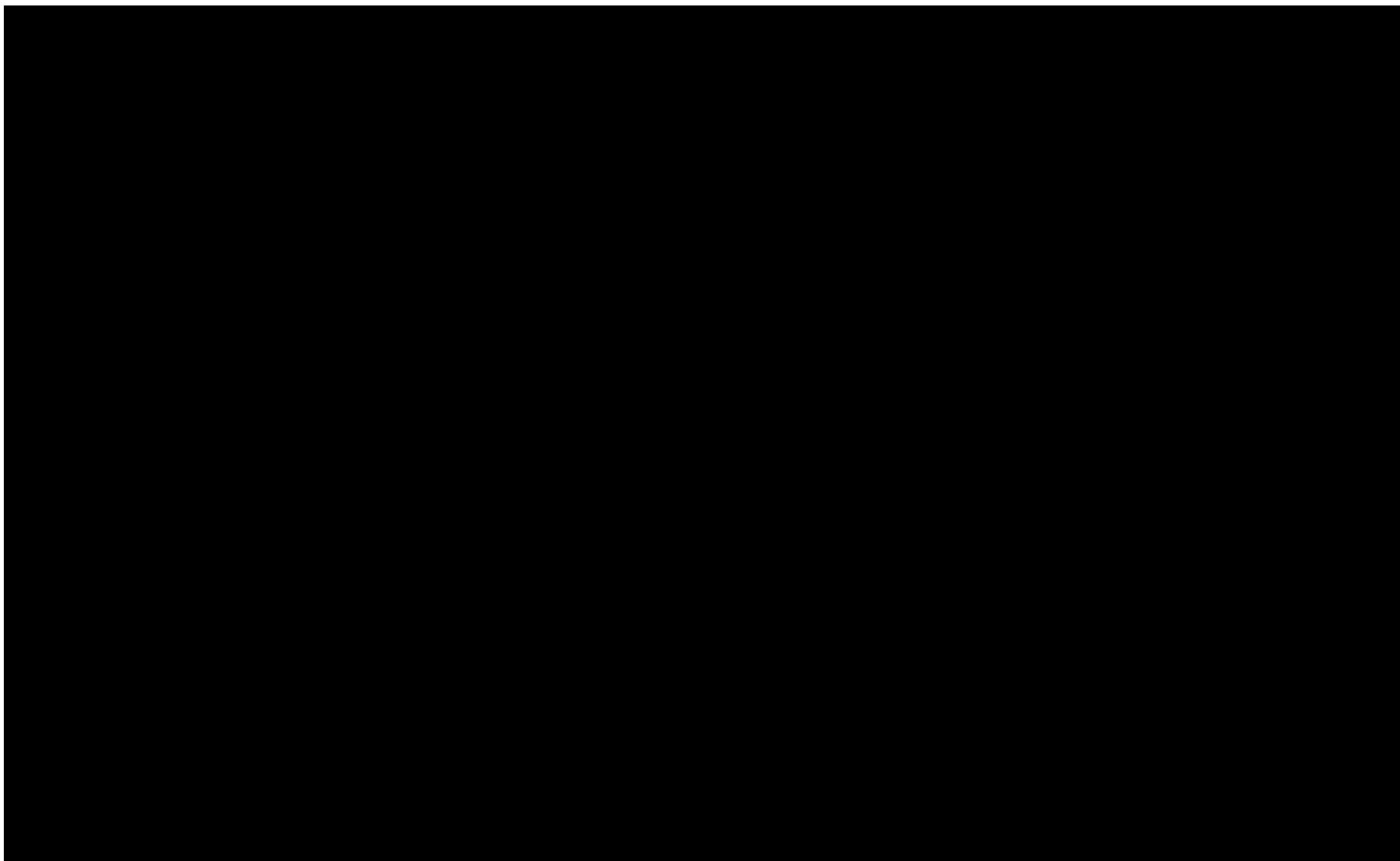


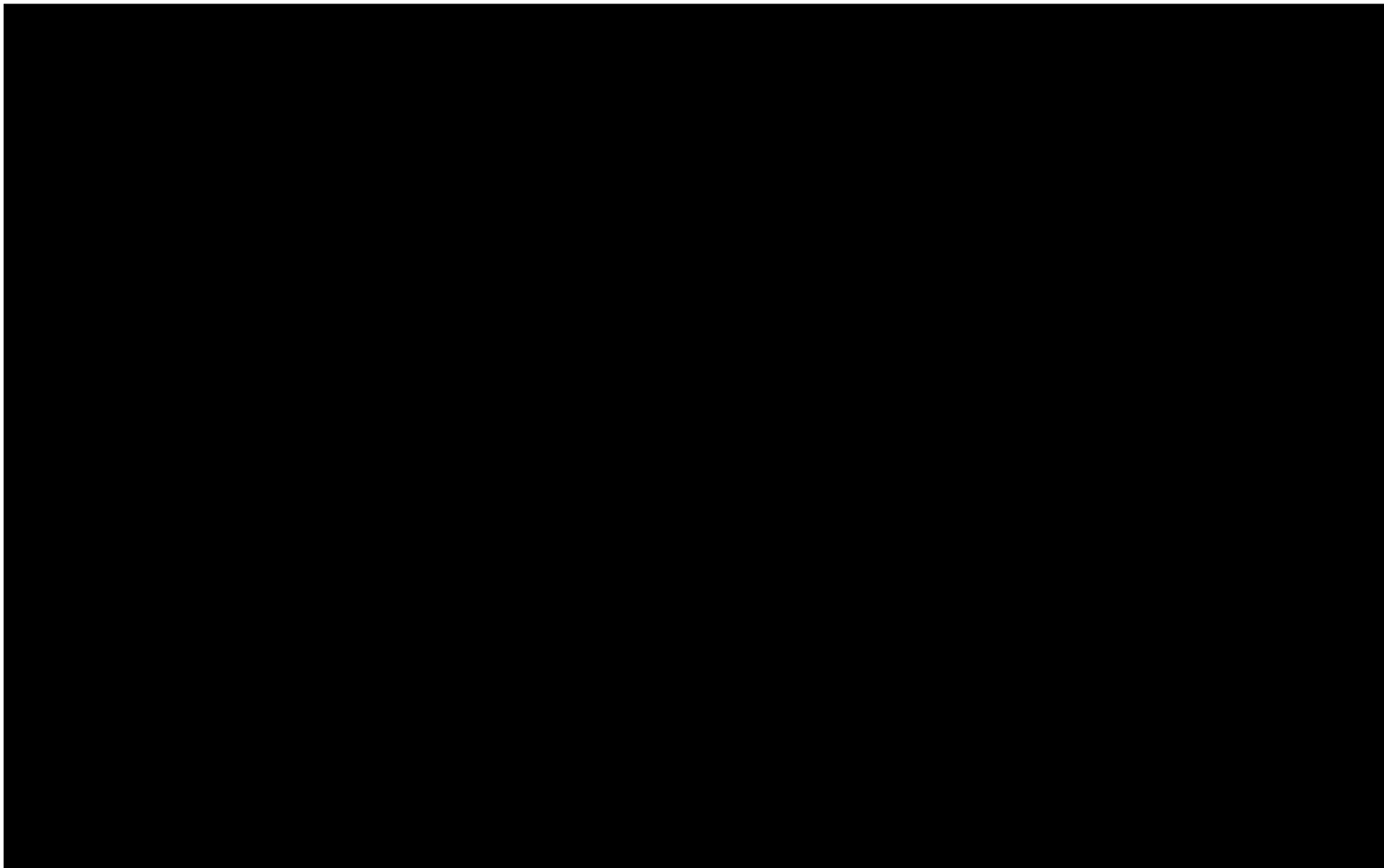


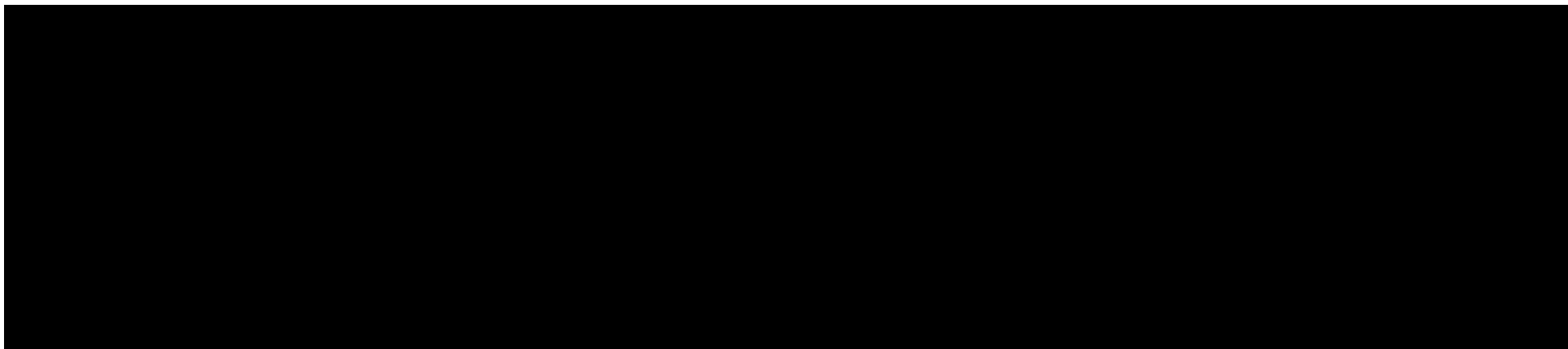












3.2 OBJECTIVES OF THE CCR DATA PROCESSING SYSTEM

The purpose of the CCR system is to provide a centralised repository for credit intelligence reported by all lenders in Ireland. The key objective of the CCR is to provide a Single Borrower View (SBV) of all credit agreements relating to an individual borrower who has obtained credit from lenders (CIPs).

The CCR will contribute to consumer protection and financial stability by¹⁶:

- *Providing lenders with more comprehensive analysis of borrowers' creditworthiness;*
- *Equipping borrowers with information on their financial profile and helping them avoid over indebtedness;*
- *Giving the Central Bank better insight into financial markets and supporting several functions e.g. prudential supervision, statistics, financial stability.*

3.3 DESIGN CONSTRAINTS FOR THE CCR SYSTEM

Constraints on the design of the system related solely to the legislation which has created the CCR.

The Credit Report Act specifically mandates the legal framework within which the CBI can operate the CCR and sets down in legislation the information which must be collected, maximum retention times and other legal parameters which must be built into the system design.

- Access to the information held on the Register
 - Duty of CIPs to access the Register
 - Power of access
 - Supplementary access (subject to consultation with the ODPC and consent of the Minister of Finance)
- Retention of data on the Register
- Retention of records of access to data on the Register
- Amendments to data and notice required for CIPs
- All access is subject to Ministerial consent and consultation with the ODPC

Additionally, nothing in the Credit Reporting Act limits the operation of the Data Protection Acts 1988 and 2003.

3.4 CCR DATA MODEL



¹⁶ <http://www.centralbank.ie/press-area/press-releases/Documents/Central%20Credit%20Register%20-%20FAQs.pdf>

- **NON-PERSONAL DATA**

- Data which cannot be related to an individual (e.g. Branch Code; Contract Reference Date; Currency)

- **PERSONAL DATA – NORMAL**

- Data which could be related to an individual but only when combined with more specific unique identifiers (e.g. Surname; Forename; Address; DOB; Role of CIS)

- **PERSONAL DATA – IDENTIFIERS**

- Data which could uniquely identify an individual directly without any additional data (e.g. PPSN; Provider CIS No.)

- **PERSONAL DATA – FACILITY**

- Data which describes the financial status, performance or otherwise of an individual, but cannot be related to that individual unless combined with Personal Data- Normal or – Identifiers. Data Subjects (CISs) may consider facility data may to be more sensitive than the PPSN or other personal data once it is linked to them. There is an inherent sensitivity associated with financial data, financial performance data or data which may be perceived to cast someone in a negative light. (e.g. Contract Status; Restructured Flag; Number of payments past due)

The full data model is outlined in Appendix I

The CBI's Information Classification Policy was also considered within the PIA's classification exercise. The data fields included in the Submission Data Model is understood to align with the following Information Classification Policy categories:

CBI Classification	PIA Classification
Confidential	Personal Data – Normal Personal Data – Identifiers Personal Data – Facility
Restricted	Non-Personal Data

APPENDIX I: DETAILED CCR DATA MODEL

Submission Data

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
Header - This is included in each submission. The first row of the record submitted must be a Header or it will throw errors.				
HD1	Record Type	HD	M	
HD2	Provider Code	Credit Information Provider Code (unique code that identifies the specific Provider) This code is assigned by the CCR to the CIP	M	
HD3	File Reference Date	This is the Reference date to which are referred the data reported in the file. It could be considered as the date when provider or processor updated information on records, or when the Submission Data file was prepared	M	
HD4	Version	Version of Submission format	M	
HD5	Submission Type	0 = STANDARD periodical contribution 1 = CORRECTION contribution 2 = HISTORIC contribution	M	
HD6	Provider Comments	In this field the CIP can report any additional comment related to current submission file, for their own use or reference. This field is not used or considered by CCR.	NM	
Body for Record Type: INDIVIDUALS (Borrowers, Guarantor) - Stores information regarding a CIS who is an individual and or a sole trader. This information is stored if the individual is a borrower or guarantor.				
ID1	Record Type	ID	M	
ID2	Provider Code	This is the Credit Information Provider (CIP) Code that uniquely identifies that CIP on the CCR. This code will be assigned by the CCR to the CIP	M	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		and must then be entered on each Record submitted.		
ID3	Branch Code	This is the code of the specific branch of the CIP sending in the record. This code is assigned by the CCR to the CIP Branch and must then be entered on each Record submitted thereafter. This code will only apply where a CIP is sending in data to the CCR through its branches.	NM	
ID4	CIS Reference Date	This is the value date for the data reported in this Record. It should represent the last date on which the Credit Information Subject (CIS) data provided in the record, was updated. If this date is not known or available, the date included as the "File Reference Date" in the Header Section, should be reported.	M	
ID5	Provider CIS No	This is the unique No. assigned by the CIP to the CIS. Each CIS must have a unique No., assigned to it by the CIP.	M	
ID6	Forename	First Name of the CIS	M	
ID7	Surname	Last Name of the CIS	M	
ID8	Gender	The Gender of the CIS	NM	
ID9	Date of Birth	The Date of Birth of the CIS	M	
ID10	Title	The Title of the CIS	NM	
ID11	Institutional Sector	A flag to indicate the ESA (European System of Accounts) category that this CIS falls under, e.g. Household other than	NM	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		Sole Proprietors, Non-profit institutions serving households etc.		
ID12	Deceased flag	Flag which indicates if a CIS is deceased.	NM	
ID13	Address 1: Address Type	This field will indicate if the Address reported is the Main Address of the CIS or an Additional Address held for the CIS.	M	
ID14	Address1: Full Address	This field should contain the complete address line including, where applicable, Apt No., House No./Name, Street Name, Village, Town, City, Postal Code etc.	D	
ID15	Address 1: Address Line1	Address Line1: First line of the Address (to include Apt/House No. where relevant)	D	
ID16	Address 1: Address Line2	Address Line2: Second line of the Address (to include Street Name and No.)	D	
ID17	Address 1: City/Town	City/Town	D	
ID18	Address 1: County	County	D	
ID19	Address 1: PostalCode	Postal Code	D	
ID20	Address 1: Country	Country	D	
ID21	Address 1: Eircode	Eircode	NM	
ID23	Address 2: Address Type	This field will indicate if the Address reported is the Main Address of the CIS or an Additional Address held for the CIS.	D	
ID24	Address2: Full Address	This field should contain the complete address line including, where applicable, Apt No., House No./Name, Street Name, Village, Town, City, Postal Code etc.	D	
ID25	Address 2: Address Line2	Address Line1: First line of the Address (to	D	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		include Apt/House No. where relevant)		
ID26	Address 2: Address Line2	Address Line2: Second line of the Address (to include Street Name and No.)	D	
ID27	Address 2: City/Town	City/Town	D	
ID28	Address 2: County	County	D	
ID29	Address 2: PostalCode	Postal Code	D	
ID30	Address 2: Country	Country	D	
ID31	Address 2: Eircode	Eircode	NM	
ID33	Identification 1: Type	Identification code type	D	
ID34	Identification 1: Number	Identification code Number	D	
ID35	Identification 2: Type	Identification code type	D	
ID36	Identification 2: Number	Identification code Number	D	
ID37	Contact 1: Type	Contact Type: Mobile Number, Landline...	D	
ID38	Contact 1: Value	Contact Value	D	
ID39	Contact 2: Type	Contact Type: Mobile Number, Landline...	D	
ID40	Contact 2: Value	Contact Value	D	
Body for Record Type: INSTALMENTS - CONTRACTS - This record is used to store information regarding instalment contracts which are: personal or business loans, leasing, mortgage loan or goods credit.				
CI 1	Record Type	CI	M	
CI 2	Provider Code	This is the Credit Information Provider (CIP) Code that uniquely identifies that CIP on the CCR. This	M	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		code will be assigned by the CCR to the CIP and must then be entered on each Record submitted.		
CI 3	Branch Code	This is the code of the specific branch of the CIP sending in the record. This code is assigned by the CCR to the CIP Branch and must then be entered on each Record submitted thereafter. This code will only apply where a CIP is sending in data to the CCR through its branches.	NM	
CI 4	Contract Reference Date	This is the value date for the data reported in this Record. It should represent the last date on which the Contract Data provided in the record, was updated. If this date is not known or available, the date included as the "File Reference Date" in the Header Section, should be reported.	M	
CI 5	Provider CIS No.	This is the unique No. assigned by the CIP to the CIS. Each CIS must have a unique No., assigned to it by the CIP.	M	
CI 6	Role of CIS	The Role of the CIS within this Contract. The values in this Domain are: - B - Borrower: A CIS who is the sole party to a credit application/agreement with a CIP - C - Co-Borrower: Multiple CISs that are party to a single credit application/agreement with a CIP. Each credit application/agreement reported can have from "0" to "n" Co-	M	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		Borrowers. - G - Guarantor: A CIS who is proposing to give, or has given, a guarantee or indemnity in connection with a credit application/agreement.		
CI 7	Consumer Flag	A flag to indicate whether or not the CIS is a consumer (Consumer Credit Act 1995) in the context of the credit agreement being reported.	M	
CI 8	Provider Contract No	This is the unique No. assigned by the CIP to the credit agreement being reported. Each credit agreement reported must have a unique No. assigned to it by the CIP.	M	
CI 9	Product Type	Product Type: Personal Loan, Mortgage etc.	M	
CI 10	Contract Phase	This is the stage of the credit cycle applicable to the reported credit application/agreement. The values in this Domain are: Requested, Active, Terminated or Closed, Terminated or Closed in Advance	M	
CI 11	Contract Status	This field will capture negative events over and above a past due position: The values in this Domain include Default Flag, Revoked Credit Card, Legal Proceedings Flag, Write-off, Debt Sold to a Third Party, Previous Negative status rectified etc.	NM	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
CI 12	Currency	This is the main reference Currency of the file. All amounts in the file should be reported in the Currency specified in this field which must be Euro.	M	
CI 13	Original Currency	This is the original currency of the credit agreement, e.g. if the credit agreement is granted in USD, this field is used to indicate this.	M	
CI 14	First date of drawdown	Instalment: This date can be the date on which funds are made available to the CIS, but should be no later than the date of first drawdown.	D	
CI 15	Contract Request Date	The date on which the credit application was made to the CIP. A credit application is an application for credit made to a CIP and completed in accordance with the application process of that CIP.	D	
CI 16	Maturity Date	The planned end date, which reflects the term set out on the credit agreement.	D	
CI 17	Contract End Actual Date	The actual end date, which will reflect early (earlier than the Maturity Date) or late (later than the Maturity Date) repayment in full.	D	
CI 18	Payment Made Date	The date on which the last payment was made by the CIS.	NM	
CI 19	Restructured flag	Modification to the credit agreement that arises out of financial distress . Values for this domain include: Interest Only, Reduced Payment, Arrears Capitalisation, etc. Domain options	NM	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		will include combinations of values		
CI 20	Reorganised Credit Code	<p>When the terms of the credit agreement are modified, this field is used to indicate that the terms have changed and also to indicate if this modification has resulted in a new account being opened. The possible values for this field are:</p> <p>0 - Credit is not re-organised 1 - Credit is re-organised by simply updating the existing account. 2 - Credit is re-organised by closing the existing account and creating a new account (the system will keep a relationship between the two accounts)</p>	NM	
CI 21	Interest Rate Type	Type of interest rate attached to the credit agreement, the Domain Values include: Standard Variable, Tracker Variable, Discount Variable, Fixed Rate etc.	D	
CI 22	Interest Rate	Annualised Agreed Rate (AAR): The AAR is the interest rate that is individually agreed between a lender and its customer, converted to an annual basis and quoted in percentages per annum. The AAR is applied in cases where the interest payments that are agreed between the lender and the customer are	D	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		capitalised at regular intervals within a year, for example per month or per quarter		
CI 23	Credit Limit	Total amount of credit that may be drawn or utilised as set out on the credit agreement	M	
CI 24	Total Number of Planned Payments	The total number of planned payments to maturity of the credit agreement. This is calculated using the Repayment Frequency and the Maturity Date: If the frequency is monthly and the facility duration is 2 years, the Total Number of Planned Payments is 24, if the frequency is weekly, the total number of planned payments is 104.	M	
CI 25	Repayment Frequency	Payment Periodicity. The values in the Domain List include weekly, fortnightly, monthly, quarterly, annually, etc.	D	
CI 26	Payment Method	Method of Payment. The values in the Domain List will include cash, direct debit etc.	NM	
CI 30	Monthly Payment due	The AVERAGE monthly payment that is due from the customer, including interest and any other fee: 1. For instalments contracts with fixed payment amount and fixed frequency of payments: Periodic payment amount / Number of months If the frequency is less than 1 month: Period payment	D	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		amount * Month Multiple, i.e. 4.3 if the frequency is weekly, 2.15 is the frequency is fortnightly 2. For instalments with variable payment amount and irregular frequency = Total amount / Total Number of months The Total Number months = the months elapsed between the first instalment due date and the Maturity Date		
CI 31	Payment Made	The amount of the payment made by the CIS in the last reporting period.	NM	
CI 32	First Payment Date	This field refers to the date of the first instalment as agreed between CIP and CIS, where there is loan with a delayed first payment. If a loan is drawn down on 01/07/2016 but the CIP allows a delayed first payment date to 1/10/2016, this field will capture the 01/10/2016 date.	NM	
CI 33	Next Payment Date	The date on which the next payment is due.	NM	
CI 34	Next Payment Amount	The next amount due to be paid by the CIS.	NM	
CI 35	Outstanding Payments Number	This field represents the number of remaining payments to be made by the CIS, including any payments missed.	D	
CI 36	Outstanding Balance	This field represents the outstanding balance, inclusive of any interest or fee applied. It should contain the Amount	D	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		Past Due where applicable.		
CI 37	Number of payments past due	<p>This field represents the number of overdue payments or past due payment. A grace period of one month should be applied before reporting this field.</p> <p>This definition is under review at present. For the Pilot Stage exercise, the following definition should be used:</p> <ol style="list-style-type: none"> 1. Calculate the Amount Past Due/Payment Due 2. Round the calculated number down to the nearest whole number 	D	
CI 38	Amount past due	<p>This field represents the current past due balance (cumulative amount of missed payments). It includes any interest or fee applied. A grace period of one month should be applied before reporting this field.</p>	D	
CI 39	Days Past Due	<p>The number of days past due as at the reporting date to the CCR.</p> <p>No grace period should be included in the value reported as this field is required for CBI purposes only. Rules for reporting as under Article 178 of the CRR Regulation (EU) No. 575/2013 2 (e) : "Institutions shall have documented policies in respect of the counting of days past due, in particular in respect of the re-ageing of the facilities</p>	NM	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		and the granting of extensions, amendments or deferrals, renewals, and netting of existing accounts. These policies shall be applied consistently over time, and shall be in line with the internal risk management and decision processes of the institution"		
Body for Record Type: NON INSTALMENTS - CONTRACTS - This record is used to store information regarding Non Instalment contracts. Non instalment contracts are those facilities that belong to the contract type credit line.				
CN1	Record Type	CN	M	
CN2	Provider Code	This is the Credit Information Provider (CIP) Code that uniquely identifies that CIP on the CCR. This code will be assigned by the CCR to the CIP and must then be entered on each Record submitted.	M	
CN3	Branch Code	This is the code of the specific branch of the CIP sending in the record. This code is assigned by the CCR to the CIP Branch and must then be entered on each Record submitted thereafter. This code will only apply where a CIP is sending in data to the CCR through its branches.	NM	
CN4	Contract Reference Date	This is the value date for the data reported in this Record. It should represent the last date on which the Contract Data provided in the record, was updated. If this date is not known or available, the date included as the "File Reference Date" in the Header Section, should be reported.	M	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
CN5	Provider CIS No	This is the unique code assigned by the CIP to the CIS. Each CIS must have a specific unique code, assigned to it by the CIP.	M	
CN6	Role	The Role of the CIS within this Contract. The values in this Domain are: Borrower: A CIS who is the sole party to a credit application/agreement with a CIP Co-Borrower: Multiple CISs that are party to a single credit application/agreement with a CIP. Each credit application/agreement reported can have from "0" to "n" Co-Borrowers. Guarantor: A CIS who is proposing to give, or has given, a guarantee or indemnity in connection with a credit application/agreement.	M	
CN7	Consumer Flag	A flag to indicate whether or not the CIS is a consumer (Consumer Credit Act 1995) in the context of the credit being reported.	M	
CN8	Provider Contract No	This is a unique code assigned by the Provider to the Contract (each single Contract facility must have a specific unique code assigned internally by the CIP and used to uniquely identify the Contract)	M	
CN9	Product Type	Product Type: Overdraft...etc.	M	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
CN10	Contract Phase	This is the stage of the credit cycle applicable to the reported credit application/agreement. The values in this Domain are: Requested, Active, Terminated or Closed, Terminated or Closed in Advance	M	
CN11	Contract Status	This field will capture negative events over and above a past due position: The values in this Domain include Default Flag, Revoked Credit Card, Legal Proceedings Flag, Write-off, Debt Sold to a Third Party, Previous Negative status rectified etc.	NM	
CN12	Currency	This is the main reference Currency of the file. All amounts in the file should be reported in the Currency specified in this field which must be Euro.	M	
CN13	Original Currency	This is the original currency of the credit agreement, e.g. if the credit agreement is granted in USD, this field is used to indicate this.	M	
CN14	First date of drawdown	Non-Instalment: This date on which the non-instalment credit agreement becomes effective and the credit line is available for utilisation by the CIS.	D	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
CN15	Contract Request Date	Request Date of the Contract	D	
CN16	Maturity Date	The planned maturity date. If there is no fixed maturity date for the overdraft, this field can be populated with a date in the future, e.g. 31/12/2099	D	
CN17	Contract End Actual Date	The actual end date will reflect the date on which the overdraft was repaid and limit was cancelled/account closed.	D	
CN18	Payment Made Date	The date on which the last payment was made by the CIS.	NM	
CN19	Restructured flag	Modification to the credit agreement that arises out of financial distress . Values for this domain include: Interest Only, Reduced Payment, Arrears Capitalisation, etc. Domain options will include combinations of values	NM	
CN20	Reorganised Credit Code	When the terms of the credit agreement are modified, this field is used to indicate that the terms have changed and also to indicate if this modification has resulted in a new account being opened. The possible values for this field are: 0 - Credit is not re-organised 1 - Credit is re-organised by simply updating the existing account. 2 - Credit is re-	NM	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		organised by closing the existing account and creating a new account (the system will keep a relationship between the two accounts)		
CN21	Interest Rate Type	Type of interest rate attached to the credit agreement, the Domain Values include: Standard Variable, Tracker Variable, Discount Variable, Fixed Rate etc.	D	
CN22	Interest Rate	Annualised Agreed Rate (AAR): The AAR is the interest rate that is individually agreed between a lender and its customer, converted to an annual basis and quoted in percentages per annum. The AAR is applied in cases where the interest payments that are agreed between the lender and the customer are capitalised at regular intervals within a year, for example per month or per quarter	D	
CN23	Credit Limit	Total amount of credit that may be drawn or utilised as set out on the credit agreement	M	
CN24	Outstanding Balance	This field should contain the used amount (utilisation) of the credit line at the specific reporting date. It represents the amount of debt outstanding under the particular facility at the	D	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		moment, including interests and fees		
Body for Record Type: CREDIT CARDS - CONTRACTS - The following record is used in order to store information regarding non instalment contracts which belong to the following contract types: credit cards or charge cards.				
CC1	Record Type	CC	M	
CC2	Provider Code	This is the Credit Information Provider (CIP) Code that uniquely identifies that CIP on the CCR. This code will be assigned by the CCR to the CIP and must then be entered on each Record submitted.	M	
CC3	Branch Code	This is the code of the specific branch of the CIP sending in the record. This code is assigned by the CCR to the CIP Branch and must then be entered on each Record submitted thereafter. This code will only apply where a CIP is sending in data to the CCR through its branches.	NM	
CC4	Contract Reference Date	This is the value date for the data reported in this Record. It should represent the last date on which the Contract Data provided in the record, was updated. If this date is not known or available, the date included as the "File Reference Date" in the Header Section, should be reported.	M	
CC5	Provider CIS No	This is the unique code assigned by the CIP to the CIS. Each CIS must have a specific unique code, assigned to it by the CIP.	M	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
CC6	Role	The Role of the CIS within this Contract. The values in this Domain are: Borrower: A CIS who is the sole party to a credit application/agreement with a CIP Co-Borrower: Multiple CISs that are party to a single credit application/agreement with a CIP. Each credit application/agreement reported can have from "0" to "n" Co-Borrowers. Guarantor: A CIS who is proposing to give, or has given, a guarantee or indemnity in connection with a credit application/agreement.	M	
CC7	Consumer Flag	A flag to indicate whether or not this credit agreements falls under the Consumer Credit Act 1995.	M	
CC8	Provider Contract No	Credit ID No. Unique Code assigned by the Provider to the Contract (each single Contract facility must have a specific unique code assigned internally by the CIP and used to uniquely identify the Contract) For Credit Cards, the Contract ID Number must not be the Credit Card number written on the card. CIPs must either send the account number linked to the Credit Card or if this is not possible, a scrambled version of the Credit Card number. The scramble algorithm applied to a	M	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		specific credit card number must return always the same code.		
CC9	Product Type	Product Type: Credit Card, Credit Card - Shared Limited, Charge Card	M	
CC10	Contract Phase	This is the stage of the credit cycle applicable to the reported credit application/agreement. The values in this Domain are: Requested, Active, Terminated or Closed, Terminated or Closed in Advance	M	
CC11	Contract Status	This field will capture negative events over and above a past due position: The values in this Domain include Default Flag, Revoked Credit Card, Legal Proceedings Flag, Write-off, Debt Sold to a Third Party, Previous Negative status rectified etc.	NM	
CC12	Currency	This is the main reference Currency of the file. All amounts in the file should be reported in the Currency specified in this field which must be Euro.	M	
CC13	Original Currency	This is the original currency of the credit agreement, e.g. if the	M	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		credit agreement is granted in USD, this field is used to indicate this.		
CC14	First date of drawdown	Credit Card: This date on which the credit card agreement becomes effective and the credit card is available for utilisation by the CIS.	D	
CC15	Contract Request Date	Request Date of the Contract	D	
CC16	Maturity Date	The planned maturity date. If there is no fixed maturity date for the credit card, this field can be populated with a date in the future, e.g. 31/12/2099	D	
CC17	Contract End Actual Date	The actual end date will reflect the date on which the credit card was repaid and account closed.	D	
CC18	Payment Made Date	The date on which the last payment was made by the CIS.	NM	
CC19	Restructured flag	Modification to the credit agreement that arises out of financial distress . Values for this domain include: Interest Only, Reduced Payment, Arrears Capitalisation, etc. Domain options will include combinations of values	NM	
CC20	Reorganised Credit Code	When the terms of the credit agreement are modified, this field is used to indicate that the terms have changed and also to indicate if this modification has resulted in a new account being opened. The possible values for this field are: 0 - Credit is not re-organised 1 - Credit is re-	NM	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		organised by simply updating the existing account. 2 - Credit is re-organised by closing the existing account and creating a new account (the system will keep a relationship between the two accounts)		
CC21	Interest Rate Type	Type of interest rate attached to the credit agreement, the Domain Values include: Standard Variable, Tracker Variable, Discount Variable, Fixed Rate etc.	D	
CC22	Interest Rate	Annualised Agreed Rate (AAR): The AAR is the interest rate that is individually agreed between a lender and its customer, converted to an annual basis and quoted in percentages per annum. The AAR is applied in cases where the interest payments that are agreed between the lender and the customer are capitalised at regular intervals within a year, for example per month or per quarter	D	
CC23	Credit limit	Total amount of credit that may be drawn or utilised as set out on the credit agreement	M	

#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
CC24	Card Reference Number	<p>This field should be populated where a single Credit Card Contract has multiple Credit Cards attaching to it.</p> <p>Where two cards are provided under a single Credit Card contract, the information is recorded on the CCR as follows:</p> <p>Credit Card 1:</p> <ul style="list-style-type: none"> - Product Type = Credit Card - Shared Limit - Card Reference Number. = xyzk <p>Credit Card 2:</p> <ul style="list-style-type: none"> - Product Type = Credit Card - Shared Limit - Card Reference Number. = xyzk <p>The "Card No." must be the same for all cards which have a shared limit. Cards with the same "Card No." mean credit cards sharing the same limit.</p>	NM	
CC25	Repayment Frequency	Payment Periodicity. Values will include bullet, weekly, fortnightly, monthly, quarterly, annually, etc.	D	
CC26	Payment Method	Method of Payment. Values will include cash, direct debit etc.	NM	
CC27	Payment Made	The total amount repaid since the last reporting date	NM	
CC28	Next Payment Date	The date on which the next payment is due.	NM	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
CC29	Next Payment Amount	This field refers to the amount of the next payment due, i.e. the upcoming instalment. For Charge Cards (payable in full each month) this field represents the amount charged in the month. For Credit Cards, this amount is evaluated as a percentage of the charged amount and any outstanding amount (in case of variable Instalments) or the fixed monthly payment (in case of fixed Instalment). The Next Payment should include interests or fees, if applied.	NM	
CC30	Outstanding Balance	This field represents the outstanding balance, inclusive of any interest or fee applied. It should contain any overdue (past due) amount, where applicable. For Charge Cards it is equal to the charged amount and for Credit Card it is the actual utilised credit amount.	NM	
CC31	Number of payments past due	This field represents the number of overdue payments or past due payment. A grace period of one month should be applied before reporting this field. This definition is under review at present. For the Pilot Stage exercise, the following definition should be used: 1. Calculate the Amount Past Due/Payment Due 2. Round the calculated number	D	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		down to the nearest whole number		
CC32	Amount past due	This field represents the current past due balance (amount of overdue payments). It should include any interest or fee applied to the amount past due. A grace period of one month applies to the reporting of this field.	D	
CC33	Days Past Due	The number of days past due as at the reporting date to the CCR. No grace period should be included in the value reported as this field is required for CBI purposes only. Rules for reporting as under Article 178 of the CRR Regulation (EU) No. 575/2013 2 (e) : "Institutions shall have documented policies in respect of the counting of days past due, in particular in respect of the re-ageing of the facilities and the granting of extensions, amendments or deferrals, renewals, and netting of existing accounts. These policies shall be applied consistently over time, and shall be in line with the internal risk management and decision processes of the institution"	NM	
CC34	Charged Amount	The amount charged on the Card at the date of reporting and should reflect the total	NM	



#	Name	Description	Mandatory / Not Mandatory/ Dependent	Classification
		amount of debits as shown on the credit card statement. It is applicable both for Credit Cards and Charge Cards.		
CC35	Last Charge Date	Date when the last transaction was charged to the card and should be the last date shown on the customer's statement.	NM	
Body for Record Type: Footer - The last row (and only the last row) will ALWAYS be the Footer.				
FT 1	Record Type	FT	M	
FT 2	Provider Code	Credit Information Provider Code (unique code that identifies the specific Provider) This code is assigned by the CCR to the Credit Provider	M	
FT 3	File Reference Date	This is the Reference date to which are referred the data reported in the file. It should be the same date included in the Header as "File Reference Date"	M	
FT 4	Nr. of records	Total number of records in the file should be reported the number of record between the Header and Footer.Header and Footer itself can or cannot be included in the count	M	



APPENDIX II: UNIVERSAL PRIVACY PRINCIPLES

The starting point of a Privacy Impact Assessment (PIA) is to identify the so-called privacy principles. Based on literature research from different sources, several privacy principles are identified, which are relevant to an assessment of the design of a new system or change in existing processing of personal data or another use of existing systems and related data processing.

There are a number of generally accepted privacy principles based on the OECD principles. These principles are coloured **red**. Furthermore there are additional privacy principles used in the *Data Protection Acts*. These principles are coloured **purple**.

Responsibility / Accountability. The responsible entities also known as “controllers” take measures to implement programs to eliminate or mitigate privacy risks on strategic, tactical and operational level. Assurance of these measures includes the proof of monitoring of these risks, internal and/or external audit and potentially reporting to external stakeholders like privacy authorities or data protection regulators.

Transparency. Citizens / consumers are informed about the use of their personal data in conjunction with the technology used and are able to *control/govern* this. The individual is therefore capable of processing certain forms of abusive behaviour, and therefore if necessary is able to challenge this in court.

Purpose limitation. Personal data is only collected for pre-specified, explicit and legitimate purposes and not for further processing if this is incompatible with the data. This is a design principle for a transparent functioning information infrastructure.

Necessity and the **limitation of data collection and the use of data (data minimization)**. The establishment of an information system is focused on supporting a specific purpose. Identification and traceability of the individual takes no longer than is strictly necessary. Minimisation of the data collected to the least amount required to achieve the objectives of the information system.

Legal basis. Personal data is processed exclusively within an appropriate legal framework e.g. the *Data Protection Act* including consent, contract, legal obligation, public duty and **legitimate interest**.

The use of personal identifying numbers, such as *digital identification numbers* is often regulated by specific law. Prior to this the *Data Protection Authority* should be asked for advice, also when it involves the use of pseudo-identities.

Data Quality. Measures which guarantee the accuracy and correctness of the personal data processed within the information system.

Data Retention. Personal data is kept for no longer than is necessary to carry out the specific purpose for which it was originally obtained.

Security of Data. Appropriate technical and organizational security measures are taken against loss or any form of unlawful processing based on a risk analysis, taking into account the technical requirements and the cost of implementation of the measures. Unnecessary collection and further processing of personal data is prevented. *PET* and *PbD* are mandatory components for the security.

Privacy Enhancing Technologies (PET). A coherent system of ICT measures that protects privacy by eliminating, reducing or preventing unnecessary and / or undesired processing of personal data, without adversely affecting the functionality of the information system.

Privacy by Design (PBD). Data security including PET is part of the design of the information system architecture and is considered at each stage of the development process and beyond – e.g. the obligation applies from the design- to the management phase of the ICT. The principles of necessity, proportionality and subsidiarity are included.

Rights of Individuals. Citizens and consumers have the right to access, correct, supplement, or request deletion of their personal data or to oppose the processing method. The individual may ask which authorities have been provided with personal data and which authorities have received their personal data.

Transfers to Third Countries. Personal data shall only be passed on to a country outside the European Union (EU) and European Economic Area (EEA) if that country ensures an adequate level of privacy protection.

Recent developments in European data protection legislation (as a result of the revelations by Edward Snowden on PRISM and national government led eavesdropping) has led to a decision by the European Court of Justice (ECJ) that the “*Safe Harbor*” framework is invalid.

Changing laws and regulations in the field of processing personal data, privacy, information security, transmission and data leaks also pose a particular risk to the privacy impact. Monitoring of these changes and maintenance of privacy measures are essential.

APPENDIX III: UNIVERSAL PRIVACY RISKS

Introduction

Processing personal data can pose risks to the privacy of consumers and/or citizens. Risks are not usually standalone; some are sometimes interwoven, can strongly influence each other and therefore are difficult to consider independently. The following risks that may arise are derived from research.

The 'Data Deluge' Effect

This effect means that the amount of personal data that is available to be processed continues to grow. This phenomenon is enhanced by both technological developments, i.e. the growth of information and communication systems, as well as by the fact that individuals are increasingly able to make use of, and to react to technologies. As more data is available and exchanged across the globe, the risk to privacy increases. The "data deluge" effect is an umbrella term for the risks which are discussed below.

The Appreciation of Personal Data

The ever increasing amounts of personal information are accompanied by an increase in value in social, political and economic terms. In certain sectors, particularly online environments, personal data has become a method of payment to access online content. Recent research shows that companies tend to build extensive collections of personal data without specific purpose. This development is made possible by the rapid decrease in the cost of digital storage and is driven by the realization that personal data is an economic resource which can be exploited. Advertisers and fraudsters create a thriving market for personal data.

'Function Creep'

Function creep is the risk of shifting or altering the purposes for which personal data was originally obtained. This risk may arise where there is an ever-growing database of personal information. Over the course of time, a change in the understanding or the needs of an organization can result in changing the use of the data in a completely different way than was ever intended when the database was first constructed.

Unauthorized Use of Unique Identifying Data

Organizations, and especially governments, issue unique personal digital identifiers. The filing and processing of these unique digital identification numbers for an individual, creates unprecedented opportunities to trace people across broad social activities thereby profiling them. It also introduces the risk of (digital) identity fraud.

This can occur if a unique personal digital identifier is used to enhance the effectiveness, efficiency and reliability of accounting processes by combining it with too many other types of personal data. Identification through these digital numbers opens a gateway for the provision of services by the government to its citizens or by commercial entities to consumers, thereby increasing the risk of identity fraud. This is associated with the risk of processing secret (non-transparent) personal data. This also includes unique identifying data such as biometrics and persistent pseudo-identities that can be traced back to individuals.

As a result of these developments, citizens or consumers can be subjected to long term, unjustified and undesirable treatment. These consequences are usually irreversible and non-recoverable, increasing the long term impact to the individual. Uniquely identifiable data can easily be distributed in society; therefore the risk of its use outside its statutory borders is additionally present.

Secret (Non-Transparent) Processing of Personal Data

If the processing of personal data is not transparent to an individual it can mean that their data is held or used against their wishes or preferences and otherwise lead to unlawful processing of personal data. Individuals may not be aware of the use of their personal information, and therefore may not see its impact in wider society. They have little or no control over this. This may mean that, without being aware of it, they are in fact stigmatized and / or excluded from social or civic amenities. Should this awareness arise, it is extremely difficult for individuals to figure out what happened and therefore hard to examine the possible negative effects. It is then is very difficult or almost impossible for an individual to exercise their right to privacy. As with unlawful use of unique identifying information, the consequences may be irreversible and irreparable.

Unauthorized Processing of Personal Data outside the EU

Transfer of personal data to countries outside the EU and EEA to countries without adequate privacy protection creates the risk of unlawful processing and the inability to effect the rights of those involved.

Data Leaks / Data Loss

As a result of data leaks or other failures in information security, personal data can fall into the hands of unauthorized individuals and can result in unlawful processing.

Large databases are susceptible to data leaks and unauthorized sharing of personal data. Individuals usually have no knowledge of such data leaks and this makes them susceptible to the effects of all the above-mentioned risks, which depend on the nature and size of the data leak, and can progressively increase in size.

Other Privacy Risks

Examples of other privacy risks that may arise from one or more of the foregoing risks are again:

- **Profiling:** Profiles of people are created based on e.g. their lifestyle, spending habits, payment behaviour, eating habits which means that they can be divided into social classes or in some way they are treated in society;
- **Incorrect treatment in society** due to errors and non-transparent processes;
- **Stigmatization** by linking data
- **Reversal of the burden of proof** on the person because the relevant data simply exists in a database and are judged by the responsible person as correct;
- **Individuals are forced to agree** to the use of their personal data for various purposes such as for obtaining services, favours or direct marketing purposes;
- New developments such as "**cloud computing**" since the digital space for personal data and applications is managed by many different (sub) processors on several system layers and across the globe. Data is moved on a regular basis, which means the relevant jurisdiction changes.
- **Activities of intelligence, surveillance and monitoring services.** Military, national security, internal and external intelligence and monitoring services undermine the security of systems and privacy principles. Security and transparency is undermined and a significant accumulation and combination of data can be realized, thereby creating non-transparent and hidden hotspots. Additionally, intelligence services can deploy malware which sabotages security and services providers may be compromised.

APPENDIX IV: RELEVANT LEGISLATION, REGULATIONS AND REFERENCE MATERIAL

Irish Legislation and Regulations

- Credit Reporting Act, 2013 (No. 45)
- Data Protection Acts 1988 and 2003
- European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011; S.I. No. 336 of 2011

European Legislation and Regulations:

- Treaty on European Union and the Treaty on the Functioning of the European Union [2012] OJ C326/01
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31
- Proposal for New EU General Data Protection Regulation, sourced from:
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Other Reference Materials

- The European Convention on Human Rights
- Personal Data Security Breach Code of Practice, approved by the Data Protection Commissioner under Section 13 (2) (b) of the Data Protection Acts, 1988 and 2003