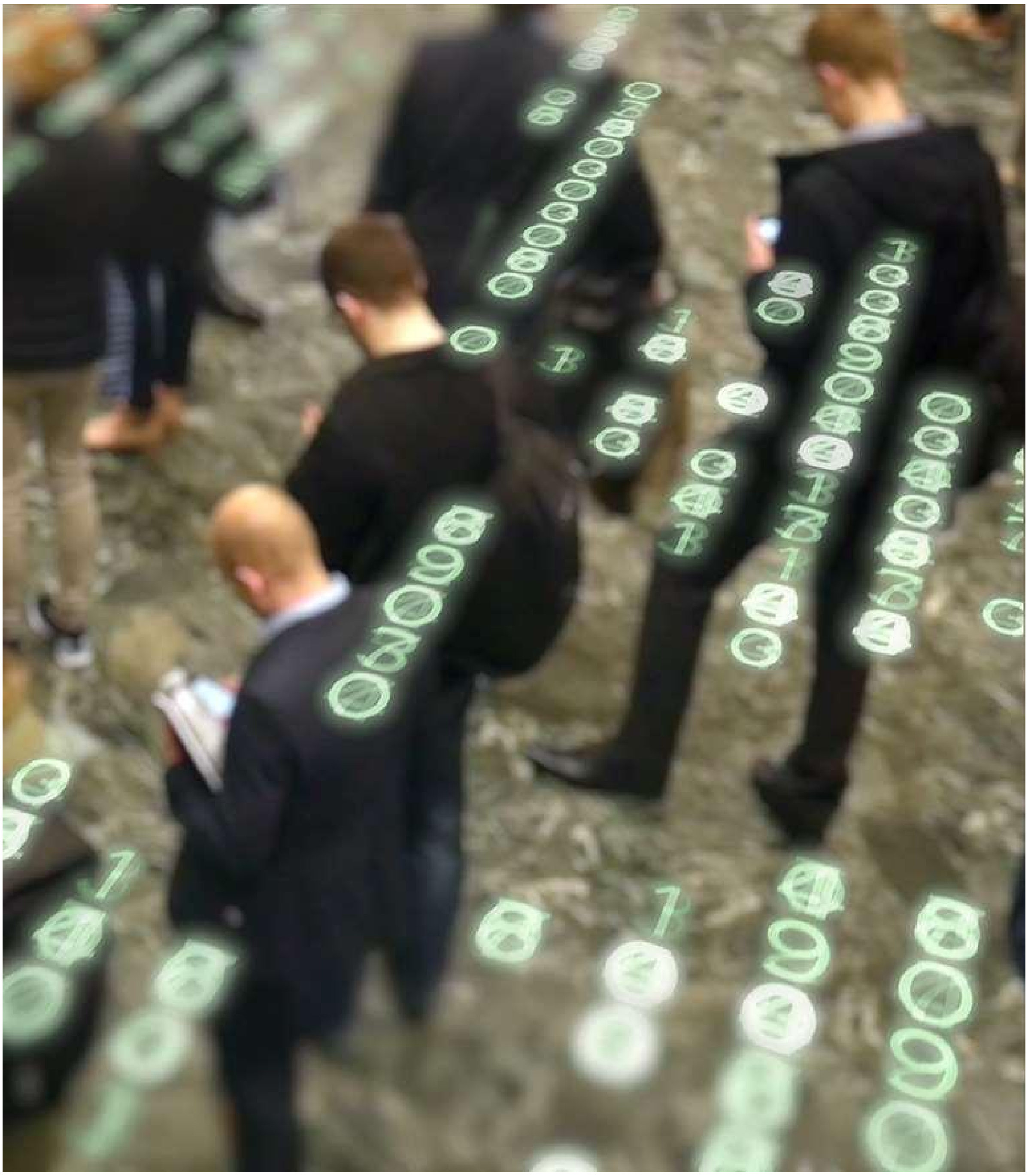
Data Protection Impact Assessment - Central Credit Register Phase 2

April 2019

Version 1.0



Central Bank of Ireland - CONFIDENTIAL

Version 1.0

DOCUMENT CONTROL

Version	Author(s)	Purpose / Change(s)	Date
1.0	Mazars	Version 1.0 prepared for CBI	10/04/2019

DOCUMENT APPROVAL

Version	Role	Name	Title	Signature	Date
v 0 x	*Reviewer / Approver*	*AN Other*	*Title, Organisation*	*Signature*	*DD/MM/YYYY*

Version 1.0

TABLE OF CONTENTS

Glossary of Terms

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

Pseudonymisation	Processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
Anonymisation	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, enacted 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, enacted in 2018, which mandates for the protection of personal data.
Data Quality	The level of quality of data. High quality data can be considered fit for purpose, and can be used to make decisions.
Subject Access Request (SAR)	Under Article 15 of the GDPR, 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 organisation, 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 Organisation for Standardisation (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.
[redacted]	[redacted]
NAMA	National Asset Management Agency
Office of the Data Protection Commission (DPC)	The DPC is an independent body responsible for upholding the rights of individuals as set out under Irish data protection legislation. The Commission is appointed by Government.
Personal Public Service Number (PPSN)	The Personal Public Service Number is a unique reference number issued by the Department of Employment Affairs and 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.
Data Protection Impact Assessment (DPIA)	A tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. It should help an organisation to identify and reduce the data protection 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.
[redacted]	[redacted]

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 DPIA

1.1.1 CCR Background

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 centralisation 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 Commission ("DPC") 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 apply to over 500 lenders, such as banks, credit unions, local authorities, NAMA, asset finance houses and moneylenders.

The CBI and CIPs separately perform Data Controller roles, with each being responsible for the data processed within its environments. The CBI is the 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 are Data Controllers for the data that they provide to the CCR. There are two sets of obligations to the data subjects, one under the Act and the other under Data Protection Law (Data Protection Act[1] and General Data Protection Regulation[2] ("GDPR")).

CRIF Ireland Limited operate the CCR and is the Data Processor on behalf of the CBI, and the CBI is responsible for ensuring that data is processed in line with the obligations outlined in the Data Protection Act, 2018, GDPR and the 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.

The Central Bank is implementing the CCR on a phased basis.

- Phase 1 focused on collecting information relating to consumer credit. A Privacy Impact Assessment (PIA) was conducted for Phase 1 for which fieldwork took place during the period September to November 2015.

- Phase 2 will focus on reporting non-consumer credit e.g. sole traders, partnerships, companies and other incorporated bodies and the development of [redacted] pseudonymised data [redacted]

1.1.2 Data Protection Impact Assessment

Article 35 of the GDPR formalises the process for the completion of a Data Protection Impact Assessment ("DPIA"), as does Directive (EU) 2016/680 and are designed to describe the processing, assess the necessity and proportionality of processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

[1] Data Protection Act, 2018

[2] EU General Data Protection Regulation

Version 1.0

A DPIA is a process of systematically considering the potential impact a project or proposed change will have on the rights and freedoms of natural persons. By completing a DPIA during a project it is possible to not only identify processing which is likely to result in a high risk to the rights and freedoms of natural persons, but also to address such issues during the project lifecycle. Given this early consideration of such risks and the ability to address such issues during the project stage, DPIA's enable privacy by design.

Pre GDPR-organisations who were mindful of privacy and data protection when implementing new projects may have completed a PIA for relevant projects. However, PIAs were not mandatory in law. The GDPR recognised and formalised the process. The approach to a PIA and DPIA is the broadly the same (Identify the need; map the data flows; identify the risks; mitigate the risks). Specifically, the GDPR:

- Makes a DPIA mandatory in certain cases;
- Requires the involvement of the DPO where one is appointed;
- Requires the supervisors to give direction on where DPIAs, and for this direction to be consistent with other EEA jurisdictions;
- Introduces compliance with an approved code of conduct as a support for the DPIA;
- Encourages the controller to seek the views of data subjects during a DPIA;
- Requires consultation with the Supervisor where the controller cannot address high risks but still wants to proceed with the processing.

The output from a PIA and DPIA remains largely consistent. Additionally, PIAs were completed prior to GDPR and compliance with GDPR is required as part of a DPIA. This introduces additional risks associated with the change from the consolidated 2003 Data Protection Act to the 2018 Data Protection Act.

The fieldwork for this DPIA took place during the period July to October 2018. The findings are based on the design as it was known and communicated to us at that point. If the design changes post the DPIA or additional information becomes available, this should be reviewed and considered in the context of its possible impact on the DPIA findings.

1.1.3 CCR Phase 1 PIA

The PIA identified nineteen privacy risks within the early phase of project design. These risks were reported to the CCR Project for consideration. A desk based review of actions taken by CBI to mitigate against risks identified was carried out in June 2017 with a follow up in March 2018. The conclusions of the review was based on conversations with management, copies of reports / guidance documentation. All items were closed on completion of the follow up testing.

1.1.4 CCR Phase 2 DPIA

It was agreed that Phase 2 should not result in a material different solution, i.e.:

- The same data flows, technology platform, underlying infrastructure, system of controls and processes will be used in Phase 2 as were designed and implemented in Phase 1.
- Whilst additional CIPs, CISs (some of whom are data subjects) and credit products are being introduced, the conclusions of the Phase 1 PIA do not appear to be materially impacted. There is no significant additional personal data being processed that wasn't considered as part of Phase 1.

[redacted] pseudonymised data [redacted] was not included in the scope of the Phase 1 PIA. A DPIA was recommended to be completed for Phase 2 in order to maintain the robust approach that has been taken to data protection over the life of the project.

The decision to undertake a DPIA is an indication of the CBI's commitment to limit the impact on individual's privacy resulting from the establishment of the CCR, as well as processing data in compliance with the applicable Data Protection Laws.

1.1.5 Key Abbreviations

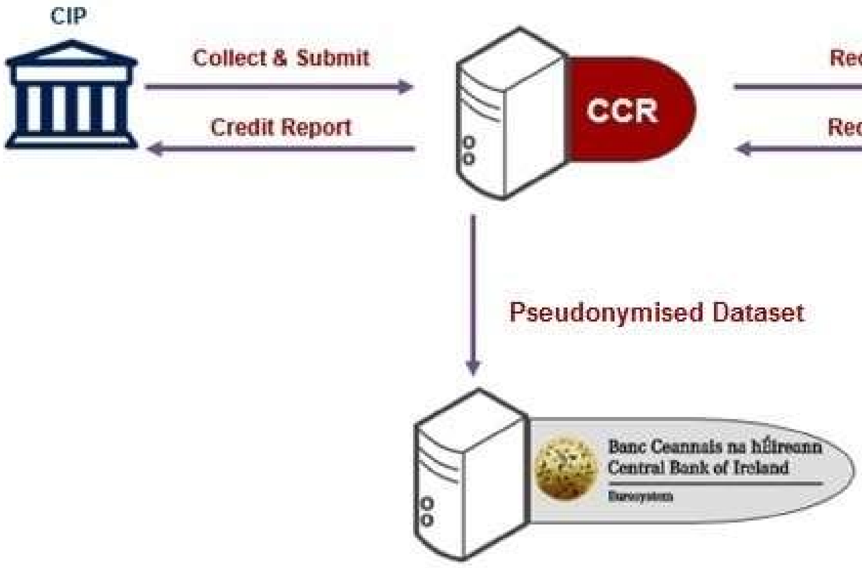
The following abbreviations are used throughout this document:

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

1.1.6 High Level Data Flows

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

High Level Data Flow Overview



The following high-level data diagram depicts [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

1.1.7 Classification of the Data in the CCR

The PIA for Phase 1 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 Act:

- **NON-PERSONAL DATA**
  - Data which cannot be related to an individual (e.g. Secondary Provider 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 Event; Number of payments past due)

A number of additional data fields were included in Phase 2. These were classified using the same categories and can be found at Appendix II.

1.2 PURPOSE, SCOPE AND APPROACH OF DPIA

1.2.1 Purpose

The purpose of the DPIA is to assess the impact that the introduction of the CCR Phase 2 will have on an individual CIS's privacy, including the protection of their data in line with applicable data protection Laws, 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 and consider privacy risks throughout the project development.

1.2.2 CCR Phase 2 DPIA Scope

The scope of the DPIA is limited to the changes in personal data processing resulting from Phase 2 of the CCR.

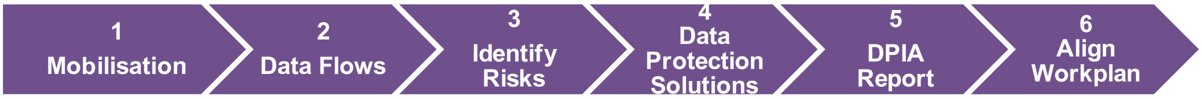
Phase 2 of the CCR extends the scope of the CCR to include non-consumer credit products and additional CISs e.g. business, corporate loans, soletraders and partnerships. While the CCR Phase 2 is collecting data (to identify person as a director of a company in order to request the company credit report; credit agreements will contain personal data for Sole Traders and possibly for partnerships), these records were considered and it was deemed that there were no significant incremental risks from Phase 1.

The PIA completed for Phase 1 of the CCR reviewed the data flows, technology platform, underlying infrastructure, system of controls and processes involved with the implementation and maintenance of the CCR. Following discussions with the CBI, we were informed that these will be the same for Phase 2. As a result, these will be deemed out of scope for Phase 2.

However, the inclusion of [redacted] pseudonymised data [redacted] was not included in the scope of the Phase 1 PIA. [redacted] will be the focus of the DPIA.

1.2.3 Approach

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



1. **Mobilisation:** 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 designed and implemented in Phase 1 to ensure they are still applicable for Phase 2. [redacted]

3. **Identify Risks:** Identification of data protection related risks associated with the one-way transfer of data between CCR and CBI.

4. **Data Protection Solutions:** Review potential solutions and set out recommendations for managing identified data protection risks.

5. **Reporting:** Prepare and document the DPIA report.

6. **Align Work Plan:** Alignment of the recommendations with and incorporate actions from DPIA into overall CCR Phase 2 Project Plan.

1.2.4 DPIA Stakeholders

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

#	Name
1	CBI CCR Project Team
2	CBI Internal Divisions / Functions (Chief Economist/Irish Economics Analysis Division, Chief Economist/Statistics. Financial Stability/Macro Financial Division. Credit Institutions Supervision/Banking Supervision Analysis, Credit Institutions Supervision/Registry of Credit Unions)
3	CBI Data Operations Function
4	CRIF Ireland Limited

Article 35(9) of the GDPR states that, where appropriate, a controller shall seek the views of data subjects or their representatives on the intended processing. Data subjects were not engaged with during Phase 2 DPIA since they were engaged as part of Phase 1 with no substantial changes being implemented in Phase 2. Additionally, data subjects view the CCR as part of the CBI, thus updating current privacy notices should suffice to meet transparency requirements.

1.3 STRUCTURE OF THE DPIA

This document is set out in the following structure:

Chapter 1: Introduction:

Introduces the concept of a DPIA, outlines the approach and principles against which the impact to an individual's privacy and protection of their data was assessed and clearly defines the scope boundaries of the assessment.

Chapter 2: Findings Summary and Data Protection Principles

Summarises the primary findings identified by the DPIA across the seven data protection principles, as outlined in the GDPR, 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. [redacted]

1.4 ACKNOWLEDGEMENTS AND USE OF THIS REPORT

Mazars was engaged by the Central Bank to complete this DPIA. 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

April 2019

2 FINDINGS

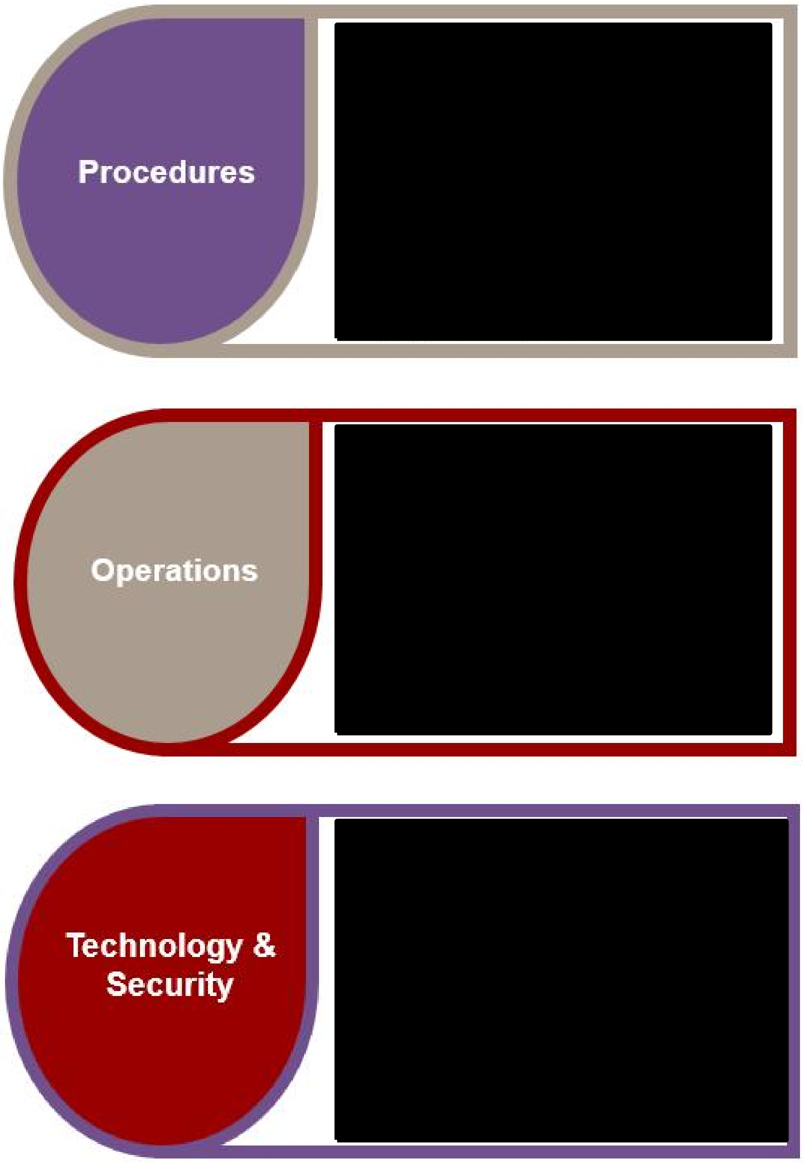
2.1 INTRODUCTION

In Ireland, the GDPR and Data Protection Act, 2018 provide 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, specifically the use of CCR by CBI for 'any of its functions' as permitted in the Act.

2.2 PRIVACY PROTECTION MEASURES WITHIN THE DESIGN

We undertook the following positive privacy measures during Phase 1 of the CCR which will remain for Phase 2:



Procedures

[redacted]

Operations

[redacted]

Technology & Security

[redacted]

Version 1.0

The completion of this DPIA for Phase 2 maintains the robust approach that has been taken to privacy and data protection over the life of the project.

2.3 FINDINGS

We have captured the data protection risks associated with the CCR under each of the seven data protection principles, (as outlined in the GDPR) listed below.

2.3.1 Data Protection Principles

Principle	Description
Lawfulness, Fairness and Transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose Limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data Minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability	The controller shall be responsible for, and be able to demonstrate, compliance with the GDPR.

An assessment of the necessity and proportionality of the processing in relation to the purposes was considered under the principles of Purpose Limitation, Data Minimisation and Storage Limitation.

Additionally, risks to the rights and freedoms of data subjects were assessed throughout the risk identification process.

2.4 DATA PROTECTION PRINCIPLE: LAWFULNESS, FAIRNESS AND TRANSPARENCY

2.4.1 Situation

The Act 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.

Section 15(7) of the Act states that "*the Bank may use any information held on the Register in the performance of any of its functions*".

The following additional Irish and EU legislation relating to the right to privacy and protection of personal information also need to be considered within the delivery and operation of the CCR, including any use of CCR data by the CBI in the performance of any of its functions:

- The Data Protection Act (2018)[3] mandates the protection of personal information relating to individuals and obliges Data Controllers to ensure the security of personal data they collect and process.

- EU General Data Protection Regulation[4].

The principle of transparency requires that it should be transparent to CISs that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

2.4.2 Findings

The Act, sets out a clear legal basis for collection and processing of personal and credit information on the CCR, including the further processing of this information by the CBI in the performance of any of its functions if there is a statutory purpose for doing so.

It lays down rules for collection, access, use and retention of personal data and credit information, together with obligations to inform CISs, to allow them access their records and to seek rectification of errors. However, CIPs currently only inform CISs that data is provided to the CCR and used to assist in the assessment of a CISs creditworthiness, and not any information regarding any further processing and use of this data by the CBI.

Risk	Impact	Recommendation
2.4.2.1 Insufficient Information provided to CISs Chapter 9 of the "Guidance on the Central Credit Register for Credit Information Providers" outlines the information CIPs are required to provide to CISs, as outlined in the Act, including: ▪ CISs rights under the Act ▪ a notice stating that the Act requires the	The information to be provided to CISs, as outlined in the Act, does not meet the requirements of Articles 12 – 14 of the GDPR. There is a risk that CISs may not be aware that the CBI intend to use CISs data for purposes other than the purposes for which data was initially captured.	CBI should update the guidance provided to CIPs to include the additional information to be provided to CISs. Information provided to CISs should be broad enough so as the notices don't

[3] Data Protection Act, 2018

[4] EU General Data Protection Regulation

Risk	Impact	Recommendation
provision of information to the CCR (specific wording provided in the Act)	Information should be provided to CISs at the time of data collection.	have to be updated constantly.

CBI Management Response

Agreed Actions:

[redacted]

[redacted]

Update the CCR Website [redacted]

Update the guidance to CIPs with regard to Section 23 and Section 24 linking to website where up to date information will be maintained.

Consideration has been given to writing to all CISs to further inform them of the use of data by CBI. In our opinion, this would constitute over-processing of personal information held on the CCR. [redacted]

Target Date for Implementation:

In advance of [redacted]

Person Responsible:

CCR Head Of Function.

2.5 DATA PROTECTION PRINCIPLE: PURPOSE LIMITATION

2.5.1 Situation

The Act, in addition to mandating the Bank to run the CCR, also makes provision that *"the Bank may use any information held on the Register in the performance of any of its functions"*.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- Section 32(3)(a) of the Act provides a gateway but not an obligation for the Bank to share information if required or permitted by law or any enactment other than the Act. The Bank will adhere to the guidelines issued by the Office of the Data Protection Commission in relation to requests from other public bodies for access to information stored on the Register. [redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2.5.2 Findings

Risk	Impact	Recommendation
2.5.2.1 CBI functions have not yet defined the purposes for which they will be processing the CCR data [redacted]	[redacted]	[redacted]
CBI Management Response Agreed Actions: [redacted] Target Date for Implementation: 31/03/2019 Person Responsible: CCR Head of Function.		

Risk	Impact	Recommendation
2.5.2.2 Other Government Agencies or State Bodies may request access to CCR data held by CBI Other government agencies /state bodies may request access to the CCR data. While the CBI will adhere to the guidelines issued by the Office of the Data Protection Commission in relation to requests from other public bodies for access to information stored on the Register, there is a risk that pseudonymised data may not be afforded that same protection.	There may be benefits to the state in being able to use pseudonymised data [redacted] However, it would also be a breach of the principle of only using personal data for the purposes it was provided. As above, a data subject may not be aware that his/her data will be shared with a third party. It is noted that the risk of government agencies /state bodies requesting access to data held on the CCR was mitigated against following the Phase 1 PIA via the implementation on a policy and procedure document.	Review policies and procedures to ensure pseudonymised data [redacted] is included with regards to accessing the CCR data.
CBI Management Response Agreed Actions: [redacted] Target Date for Implementation: Already implemented. Person Responsible: n/a		

2.6 DATA PROTECTION PRINCIPLE: DATA MINIMISATION

2.6.1 Situation

[redacted]

[redacted]

2.6.2 Findings

Risk	Impact	Recommendation
2.6.2.1 Each CBI function requires different subsets of the CCR data set [redacted]	[redacted]	[redacted]
CBI Management Response Agreed Actions: [redacted] [redacted] Target Date for Implementation: In advance of [redacted] Person Responsible: CCR Head Of Function.		

Risk	Impact	Recommendation
2.6.2.2 Combining current CBI datasets with the CCR to identify data subjects [redacted]	[redacted]	[redacted]
CBI Management Response Agreed Actions: [redacted] Target Date for Implementation: March 2019. Person Responsible: CCR Head Of Function.		

2.7 DATA PROTECTION PRINCIPLE: ACCURACY

2.7.1 Situation

The accuracy and quality of data is the responsibility of the CIPs who will provide the data to the CCR for matching, scoring and processing. However, the CCR perform routine and automated data quality checks to assess the accuracy, correctness and quality of the personal data loaded onto the CCR database.

Submission:

- The CCR 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.
  - A CCR operator reviews the output log from each validation step above and can proceed to load the file into the database, or stop processing due to the number of errors identified according to the internal data quality policies defined by the CCR. 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 from the staging area into the CCR database.

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.

Rectification of inaccurate data in CCR

The Act 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.

It should also be noted that:

- 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 established to allow a CIP request the CCR to amend information urgently on the CCR rather than wait for submission of amendment

Data stored in CCR compared to that accessed by CBI functions

On a monthly basis, each CIP submits changes to personal and all facility data relating to CISs with credit agreements to the CCR. Additionally, on each enquiry to the CCR, a CIP submits relevant personal and facility data to identify a CIS and match to any existing records on the CCR. As a result, information stored on the CCR is live, i.e. it reflects the latest information submitted by CIPs.

[redacted]

2.7.2 Findings

[redacted]

The risks highlighted are unlikely to have a negative impact on the data subjects, thus the risk to the rights and freedoms of a data subject is not significant.

CBI Management Response

None required

2.8 DATA PROTECTION PRINCIPLE: STORAGE LIMITATION

2.8.1 Situation

Section 8 of the Act outlines the following periods for which information may be held on the Register:

- Personal information and credit information which identifies a CIS relating to a credit application may be held for 6 months
- Credit information which identifies a CIS and is held on the Register as the result of a credit agreement may be held on the Register until the end of the period of 5 years beginning with the first day on which all liabilities under the credit agreement to which it relates have been discharged*
- Personal information which identifies a CIS and is held on the Register as the result of a credit agreement may be held on the Register for as long as any credit information relating to the credit information subject may be held on the Register
- Anonymised information may be held on the Register indefinitely

**In the case of credit information to which section 7(2)(b) applies, until the end of the period of 5 years beginning with the day on which the proposal is withdrawn or the arrangement is terminated. In the* *case of credit information to which section 5(2)(d) or 7(2)(c) applies, until the end of the period of 5 years beginning with the day on which it is entered on the Register*

Section 30(1) of the Act states that CBI may produce:

- Credit score and other analyses in relation to CISs, and
- General reports, analyses, and statistics from which CISs cannot be identified.

Where anything produced under subsection (1) is not held on the Register CBI may sell it or publish it and sell copies of it.

15(7) of the Act states *"The Bank may use any information* ***held on the Register*** *in the performance of any of its functions"*

CBI will continue to use pseudonymised data obtained from the Register beyond the retention period outlined in the Act. This data will no longer be *"held on the Register"* once the retention period has been reached. Additionally, this pseudonymised data will be held by CBI indefinitely. Over time, there is the possibility that CBI will have a substantial record of a CIS's credit worthiness/profile, i.e. if an individual has a 35 year mortgage, the personal and credit information relating to this mortgage will be retained on the CCR for the duration of the mortgage. Any additional credit applications or past credit agreements which have now exceeded the 5 year retention period will have now been removed from the CCR. However, this mortgage information will be retained in the CBI indefinitely. [redacted]

[redacted]

2.8.2 Findings

Risk	Impact	Recommendation
2.8.2.1 CBI retaining information beyond the periods for which it may be held on the Register [redacted]	[redacted]	[redacted]

Risk	Impact	Recommendation
	[redacted]	

CBI Management Response

Agreed Actions:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Risk	Impact	Recommendation
Target Date for Implementation: In advance of [redacted] Person Responsible: CCR Head Of Function.		
2.8.2.2 Each CBI function will have different retention requirements [redacted]	[redacted]	[redacted]
CBI Management Response Agreed Actions: [redacted] Target Date for Implementation: January 2019. Person Responsible: CCR Head Of Function.		

2.9 DATA PROTECTION PRINCIPLE: INTEGRITY AND CONFIDENTIALITY

2.9.1 Situation

Data processing is outsourced to CRIF which has established an Information Security Management Systems (ISMS) to protect the confidentiality, integrity, availability and authenticity of information. This ISMS is based on the ISO27001:2013 information security standard. Security of data stored and processed in the CCR was in scope for the Phase 1 PIA with a number of risks identified along with mitigating actions taken. However, the CBI has responsibility to ensure the security of all data received by the CBI from the CCR. The CBI must prevent against loss of or any form of unlawful processing of the data.

2.9.2 Findings

Risk	Impact	Recommendation
2.9.2.1 Potential for CBI employees to use the data for malicious intent [redacted]	[redacted]	[redacted]
CBI Management Response Agreed Actions: [redacted] [redacted] [redacted]		

Risk	Impact	Recommendation
[redacted] Target Date for Implementation: None. Person Responsible: CCR Head Of Function.		
2.9.2.2 Additional location of data leading to greater risk of external unauthorised access [redacted]	[redacted]	[redacted]
CBI Management Response Agreed Actions: [redacted] Target Date for Implementation: None.		

Risk	Impact	Recommendation
Person Responsible: CCR Head Of Function.		

2.10 DATA PROTECTION PRINCIPLE: ACCOUNTABILITY

2.10.1 Situation

Data Controllers

CIPs: Each CIP is a 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 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 is a data processor and processes all credit and personal information stored on the CCR under the contract with the CBI. The Bank is ultimately responsible for the activities of its data processor, CRIF Ireland Limited.

CBI approach to GDPR

The CBI undertook a separate GDPR project which addressed the obligations on the bank under GDPR. Actions resulting from this project applicable to the CCR included, but not limited to:

- All CBI colleagues have completed GDPR training
- The contract with CBI and CRIF is subject to additional GDPR addendum
- The Bank has appointed a DPO
- The Data Protection Statement on the CCR Website has been updated to reflect GDPR changes

2.10.2 Findings

CBI Management Response
None required

3 DESCRIPTION OF THE CCR SYSTEM, PROCESSES AND DATAFLOWS

3.1 PHASE 1 PIA FINDINGS

Phase 2 of the CCR implementation will not result in any material changes to systems, processes and dataflows used to implement and manage the CCR during Phase 1. A detailed outline of the CCR system, processes and dataflows can be found at Appendix I.

3.2 PHASE 2 TRANSFER OF DATA FROM CCR TO CBI

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

4 DATA PROTECTION OFFICER REVIEW

I have reviewed the DPIA performed in respect of the CCR – Phase 2 DPIA whereby it is planned that psuedonymised personal data [redacted] and have provided comments on previous drafts. [redacted] Bank is permitted under the Credit Reporting Act. The DPIA outlines the various risks under the main Data Protection principles and outlines the controls in place or planned in order to mitigate these risks. Overall, I am satisfied that the controls outlined are appropriate to the nature of the personal data being processed given that the data to be processed [redacted] will be pseudonymised.

[redacted]

I note that for CCR Phase 1 DPIA that there was formal consultation with individuals and hence there was no necessity for additional consultation for the Phase 2 DPIA. I consider that based on the mitigation plans as outlined that there are no high risks to the rights of individuals remaining which requires this DPIA to be formally submitted to the Data Protection Commission.

Tom Meade, DPO

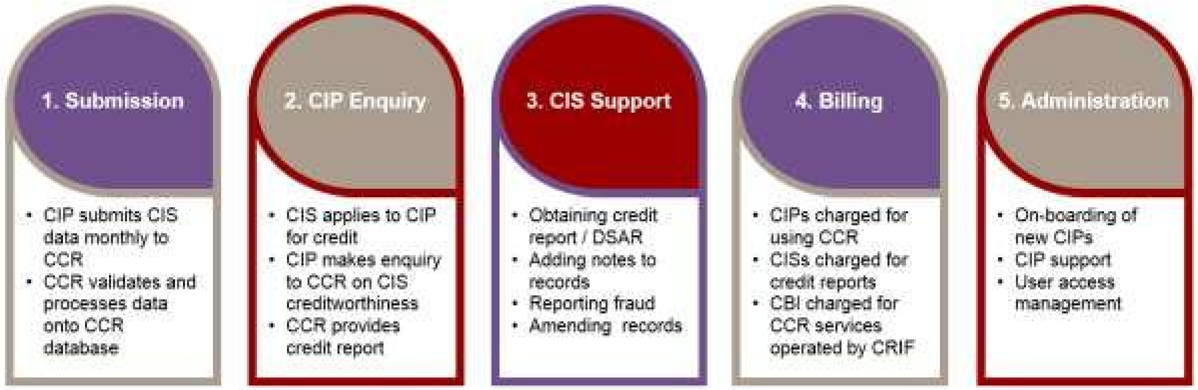
Dated: 28 March 2019

APPENDIX I: DETAILED DESCRIPTION OF THE CCR SYSTEM, PROCESSES AND DATAFLOWS

[redacted]

CCR Macro Processes

The PIA for Phase 1 assessed the following macro-processes that were introduced to manage the CCR. We prepared detailed data flows to assist the identification of data protection risks and these are below.



1. Submission

- CIP submits CIS data monthly to CCR
- CCR validates and processes data onto CCR database

2. CIP Enquiry

- CIS applies to CIP for credit
- CIP makes enquiry to CCR on CIS creditworthiness
- CCR provides credit report

3. CIS Support

- Obtaining credit report / DSAR
- Adding notes to records
- Reporting fraud
- Amending records

4. Billing

- CIPs charged for using CCR
- CISs charged for credit reports
- CBI charged for CCR services operated by CRIF

5. Administration

- On-boarding of new CIPs
- CIP support
- User access management

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

OBJECTIVES OF THE CCR DATA PROCESSING SYSTEM

- The Central Bank is committed to serving the public interest by safeguarding monetary and financial stability and working to ensure that the financial system serves the needs of the economy and its customers over the long term. The CCR will play a key role in contributing to the stability of the financial system and protecting consumers by facilitating informed credit decisions. The Central Bank uses the Register to get better insights into the overall level and patterns of lending in the economy.

CCR DATA MODEL

[redacted]

- **NON-PERSONAL DATA**
  - Data which cannot be related to an individual (e.g. Secondary Provider 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 Event; Number of payments past due)

The full CCR data model is outlined in Appendix II. [redacted]

[redacted]

The CBI's Information Classification Policy was also considered within the Phase 1 PIA's classification exercise.

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

APPENDIX II: DETAILED CCR DATA MODEL

[redacted]

Submission Data Format for Lenders

#	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	[redacted]
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	[redacted]
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	[redacted]
HD4	Version	Version of Submission format	M	[redacted]
HD5	Submission Type	0 = STANDARD periodical contribution 1 = CORRECTION contribution 2 = HISTORIC contribution	M	[redacted]
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	[redacted]
Body for Record Type: INDIVIDUALS (Borrowers, Guarantor) - Information regarding a CIS who is an individual and or a sole trader.				
ID1	Record Type	**ID**	M	[redacted]

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 and must then be entered on each Record submitted.	M	[redacted]
ID3*	Secondary Provider 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	[redacted]
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	[redacted]
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	[redacted]
ID6	Forename	First Name of the CIS	M	[redacted]
ID7	Surname	Last Name of the CIS	M	[redacted]
ID8	Gender	The Gender of the CIS	NM	[redacted]
ID9	Date of Birth	The Date of Birth of the CIS **(only the year to be transferred from CCR to CBI)**	M	[redacted]
ID11	Institutional Sector	A flag to indicate the ESA (European System of Accounts) category that this CIS falls under, e.g. Household other than Sole Proprietors, Non-profit institutions serving households etc.	NM	[redacted]
ID12	Deceased flag	Flag which indicates if a CIS is deceased.	NM	[redacted]
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	[redacted]
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. **(only county and postal code will be sent to CBI)**	D	[redacted]

ID15	Address 1: Address Line1	Address Line1: First line of the Address (to include Apt/House No. where relevant)	D	[redacted]
ID16	Address 1: Address Line2	Address Line2: Second line of the Address (to include Street Name and No.)	D	[redacted]
ID17	Address 1: City/Town	City/Town	D	[redacted]
ID18	Address 1: County	County	D	[redacted]
ID19	Address 1: PostalCode	Postal Code	D	[redacted]
ID20	Address 1: Country	Country	D	[redacted]
ID21	Address 1: Eircode	Eircode **(just the first three characters to be sent from CCR to CBI)**	NM	[redacted]
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	[redacted]
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. **(only county and postal code will be sent to CBI)**	D	[redacted]
ID25	Address 2: Address Line2	Address Line1: First line of the Address (to include Apt/House No. where relevant)	D	[redacted]
ID26	Address 2: Address Line2	Address Line2: Second line of the Address (to include Street Name and No.)	D	[redacted]
ID27	Address 2: City/Town	City/Town	D	[redacted]
ID28	Address 2: County	County	D	[redacted]
ID29	Address 2: PostalCode	Postal Code	D	[redacted]
ID30	Address 2: Country	Country	D	[redacted]
ID31	Address 2: Eircode	Eircode **(just the first three characters to be sent from CCR to CBI)**	NM	[redacted]
ID33	Identification 1: Type	Identification code type	D	[redacted]
ID34	Identification 1: Number	Identification code Number	D	[redacted]
ID35	Identification 2: Type	Identification code type	D	[redacted]

ID36	Identification 2: Number	Identification code Number	D	[redacted]
ID37	Contact 1: Type	Contact Type: Mobile Number, Landline…	D	[redacted]
ID38	Contact 1: Value	Contact Value	D	[redacted]
ID39	Contact 2: Type	Contact Type: Mobile Number, Landline…	D	[redacted]
ID40	Contact 2: Value	Contact Value	D	[redacted]
ID41	Sector of Economic Activity	Classification of CIS according to their economic activities, in accordance with the NACE rev.2 statistical classification.	NM	[redacted]
ID42	Employment:Employment Status	The employment status of the CIS. The CIP should select the most appropriate value from the domain list	NM	[redacted]
ID43	Employment:Occupation Category	The Occupation Title of the CIS. The CIP should select the most appropriate value from the domain list	NM	[redacted]
ID44	Sole Trader: TradeName	Name of the Business/Trading name of the Sole Trader.	D	[redacted]
ID45	Sole Trader Address1: 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. Please note: A default value can be set for this Domain.	D	[redacted]
ID46	Sole Trader Address 1: Full Address	This field should contain the concatenation of all address lines including, all the addresses lines such as Street name and number, City/Village, Postal Code, etc. **(only county and postal code will be sent to CBI)**	D	[redacted]
ID47	Sole Trader Address 1: Address line 1	First line of the Business Address (to include Apt/House No. or Office Block Name etc. where relevant)	D	[redacted]
ID48	Sole Trader Address 1: Address line 2	Second line of the Business Address	D	[redacted]
ID49	Sole Trader Address 1: PostalCode	Postal Code	NM	[redacted]

ID50	Sole Trader Address 2: City/Town	City/Town	D	[redacted]
ID51	Sole Trader Address 1: County	County	D	[redacted]
ID52	Sole Trader Address 1: Country	Country	D	[redacted]
ID53	Sole Trader Address 1: Eircode	Eircode **(just the first three characters to be sent from CCR to CBI)**	NM	[redacted]
ID55	Sole Trader 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	[redacted]
ID56	Sole Trader Address 2: Full Address	This field should contain the concatenation of all address lines including, all the addresses lines such as Street name and number, City/Village, Postal Code, etc... **(only county and postal code will be sent to CBI)**	D	[redacted]
ID57	Sole Trader Address 2: Address line 1	First line of the Business Address (to include Apt/House No. or Office Block Name etc. where relevant)	D	[redacted]
ID58	Sole Trader Address 2: Address line 2	Second line of the Business Address	D	[redacted]
ID59	Sole Trader Address 2: PostalCode	Postal Code	NM	[redacted]
ID61	Sole Trader Address 2: County	County	D	[redacted]
ID62	Sole Trader Address 2: Country	Country	D	[redacted]
ID63	Sole Trader Address 2: Eircode	Eircode **(just the first three characters to be sent from CCR to CBI)**	NM	[redacted]
ID65	Sole Trader: 1 Identification Type	Identification Code Type	D	[redacted]
ID66	Sole Trader: 1 Identification Number	Identification Code Number	D	[redacted]
ID67	Sole Trader: 2 Identification Type	Identification Code Type	D	[redacted]
ID68	Sole Trader: 2	Identification Code Number	D	[redacted]

	Identification Number			
Companies - non-individual (BD)				
BD1	Record Type	**CC**	M	[redacted]
BD2	Provider Code	This is the Credit Information Provider (CIP) Code that uniquely identifies the 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	[redacted]
BD4	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	[redacted]
BD5	Provider CIS No	This is the unique identifier assigned by the CIP to the CIS. Each CIS must have a unique identifier assigned to it by the CIP.	M	[redacted]
BD6	Entity Legal Name	Legal Name of the Business	D	[redacted]
BD7	Entity Trading / Business name	Entity Trading / Business name	D	[redacted]
BD8	Entity Form	Entity form is the type of Entity being reported, e.g. Limited Company, Partnership, Unincorporated Charity etc.	M	[redacted]
BD9	Sector of Economic Activity	Classification of CIS according to their economic activities, in accordance with the NACE rev.2 statistical classification	NM	[redacted]
BD10	Enterprise Size	The classification of enterprises by size, in accordance with the Annex to Commission Recommendation 2003/361/EC. Select the appropriate value from the domain list	NM	[redacted]
BD11	Institutional Sector	The value reported must align with a value in the Enterprise Size Domain	NM	[redacted]
BD12	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	[redacted]
BD13	Address1: Full Address	This field should contain the complete address line including, all the addresses lines such as Street name and number, City/Village, Postal Code, etc. **(where the entity**	D	[redacted]

		form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form only county and postal code will be sent to CBI)		[redacted]
BD14	Address 1: Address Line1	Address Line1: First line of the CIS Address (to include Apt/House No. where relevant))...**(where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form this will not be sent)**	D	[redacted]
BD15	Address 1: Address Line2	Address Line2: Second line of the CIS address (to include street Name and No.))...**(where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form this will not be sent)**	N M	[redacted]
BD16	Address 1: City/Town	City/Town)...**(where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form this will not be sent)**	N M	[redacted]
BD17	Address 1: PostalCode	Postal Code	N M	[redacted]
BD18	Address 1: County	County	D	[redacted]
BD19	Address 1: Country	Country	D	[redacted]
BD20	Address 1: Eircode	Eircode **(where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form only county and postal code will be sent to CBI)**	N M	[redacted]
BD22	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	[redacted]
BD23	Address 2: Full Address	This field should contain the complete address line including, all the addresses lines such as Street name and number, City/Village, Postal Code, etc...**(where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form only county and postal code will be sent to CBI)**	D	[redacted]
BD24	Address 2: Address Line1	Address Line1: First line of the CIS Address (to include Apt/House No. where relevant)...**(where the entity form is a group of individuals e.g.,**	D	[redacted]

		club, association, partnership, unincorporated charity, non legal form this will not be sent)		[redacted]
BD25	Address 2: Address Line2	Address Line2: Second line of the CIS address (to include street Name and No.)...**(where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form this will not be sent)**	NM	[redacted]
BD26	Address 2: City/Town	City/Town)...**(where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form this will not be sent)**	NM	[redacted]
BD27	Address 2: PostalCode	Postal Code	NM	[redacted]
BD28	Address 2: County	County	D	[redacted]
BD29	Address 2: Country	Country	D	[redacted]
BD30	Address 2: Eircode	Eircode **(where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form only county and postal code will be sent to CBI)**	NM	[redacted]
BD32	Identification 1: Type	Identification Code Type	D	[redacted]
BD33	Identification 1: Number	Identification Code Number	D	[redacted]
BD34	Identification 2: Type	Identification Code Type	D	[redacted]
BD35	Identification 2: Number	Identification Code Number	D	[redacted]
BD36	Contact 1: Type	Contact Type: Phone Number, Email, Website	D	[redacted]
BD37	Contact 1: Value	Contact Value **(Email address will not be sent for all entities. Where the entity form is a group of individuals e.g., club, association, partnership, unincorporated charity, non legal form no contact value will be sent)**	D	[redacted]
BD38	Contact 2: Type	Contact Type: Phone Number, Email, Website	D	[redacted]
BD39	Contact 2: Value	Contact Value **(Email address will not be sent for all entities. Where the entity form is a group of**	D	[redacted]

		individuals e.g., club, association, partnership, unincorporated charity, non legal form no contact value will be sent)		[redacted]
Body for Record Type: INSTALMENTS - CONTRACTS - Information regarding instalment contracts which are: personal or business loans, leasing, mortgage loan or goods credit				[redacted]
CI 1	Record Type	**CI**	M	[redacted]
CI 2*	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	[redacted]
CI 3	Secondary Provider 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	[redacted]
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	[redacted]
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. [redacted]	M	[redacted]
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-Borrowers. - G - Guarantor: A CIS who is proposing to give, or has given, a guarantee or indemnity in connection with a credit application/agreement.	M	[redacted]
CI 7	Consumer Flag	A flag to indicate whether or not the CIS is a consumer (Consumer Credit Act 1995) in the context of	M	[redacted]

		the credit agreement being reported.		[redacted]
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. [redacted]	M	[redacted]
CI 9	Product Type	Product Type: Personal Loan, Mortgage etc.	M	[redacted]
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	[redacted]
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	[redacted]
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	[redacted]
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	[redacted]
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	[redacted]
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	[redacted]
CI 16	Maturity Date	The planned end date, which reflects the term set out on the credit agreement.	D	[redacted]

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	[redacted]
CI 18	Payment Made Date	The date on which the last payment was made by the CIS.	NM	[redacted]
CI 19	Restructured Event	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	[redacted]
CI 20	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-organised by closing the existing account and creating a new account (the system will keep a relationship between the two accounts)	NM	[redacted]
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	[redacted]
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 capitalised at regular intervals within a year, for example per month or per quarter	D	[redacted]
CI 23	Financed Amount	Total amount of credit that me be drawn or utilised as set out on the credit agreement	M	[redacted]
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	M	[redacted]

		weekly, the total number of planned payments is 104.		[redacted]
CI 25	Payment Frequency	Payment Periodicity. The values in the Domain List include weekly, fortnightly, monthly, quarterly, annually, etc.	D	[redacted]
CI 26	Payment Method	Method of Payment. The values in the Domain List will include cash, direct debit etc.	NM	[redacted]
CI 27	Repayment Type	The type of amortisation applicable to the contract at the reporting date. Please select the appropriate value from the domain list	NM	[redacted]
CI 28	Purpose of Credit Type	Classification of contracts according to their purpose. Please select the appropriate value from the domain list	NM	[redacted]
CI 29	Exposure Class	Exposure Class of the credit agreement reported. Values in the domain will include Retail, Retail secured by real estate property, Retail Secured by real estate property SME etc.	NM	[redacted]
CI 30	MOF Link Code	Multi Option Facility Link is a code which links the sub facilities of a Multi Option Facility **(As this could be a very similar to the provider contract number, an alternative id to be provided to CBI)**	M	[redacted]
CI 31	Payment Made	The amount of the payment made by the CIS in the last reporting period.	NM	[redacted]
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	[redacted]
CI 33	Next Payment Date	The date on which the next payment is due.	NM	[redacted]

CI 34	Next Payment Amount	The next amount due to be paid by the CIS.	NM	[redacted]
CI 35	Outstanding Payments Number	This field represents the number of remaining payments to be made by the CIS, including any payments missed.	D	[redacted]
CI 36	Outstanding Balance	This field represents the outstanding balance, inclusive of any interest or fee applied. It should contain the Amount Past Due where applicable.	D	[redacted]
CI 37	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 down to the nearest whole number	D	[redacted]
CI 38	Amount past due	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.	D	[redacted]
CI 39	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	[redacted]
Body for Record Type: NON INSTALMENTS - CONTRACTS - Information regarding Non Instalment contracts. Non instalment contracts are those facilities that belong to the contract type credit line.				
CN1	Record Type	**CN**	M	[redacted]

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	[redacted]
CN3	Secondary Provider 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	[redacted]
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	[redacted]
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. [redacted]	M	[redacted]
CN6	Role of CIS	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	[redacted]
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	[redacted]
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) [redacted]	M	[redacted]

		[redacted]		[redacted]
CN9	Product Type	Product Type: Overdraft…etc.	M	[redacted]
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	[redacted]
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	[redacted]
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	[redacted]
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	[redacted]
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	[redacted]
CN15	Contract Request Date	Request Date of the Contract	D	[redacted]
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	[redacted]
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	[redacted]
CN18	MOF Link Code	Multi Option Facility Link is a code which links the sub facilities of a Multi Option Facility **(As this could be a very similar to the provider**	M	[redacted]

		contract number, an alternative id to be provided to CBI)		[redacted]
CN19	Restructure Event	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	[redacted]
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-organised by closing the existing account and creating a new account (the system will keep a relationship between the two accounts)	NM	[redacted]
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	[redacted]
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	[redacted]
CN23	Credit Limit	Total amount of credit that may be utilised as set out on the credit agreement	M	[redacted]
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 moment, including interests and fees	D	[redacted]
CN25	Purpose of Credit Type	Classification of contracts according to their purpose. Please select the appropriate value from the domain list	NM	[redacted]

CN26	Exposure Class	The classification of the contract in line with CRR/CRD IV IRB exposure classes. Select the most relevant domain value from the list. Within the corporate asset class: Real estate related exposures are those relating to the sales and/or letting of residential or commercial property; Other corporate refers to exposures in the COREP class Corporate which are neither SME nor Specialised Lending. Within the retail exposure class secured by real estate property: Owner Occupier refers to loans secured on residential real estate occupied by the owner Buy-to-let refers to loans secured on residential real estate rented from the owner by a third party. See Chapter 4 of the Guidance on the CCR for further information.	NM	[redacted]
Body for Record Type: CREDIT CARDS - CONTRACTS - Information regarding non instalment contracts which belong to the following contract types: credit cards or charge cards.				
CC1	Record Type	**CC**	M	[redacted]
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	[redacted]
CC3	Secondary Provider 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	[redacted]
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	[redacted]
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.[redacted]	M	[redacted]

		[redacted]		[redacted]
CC6	Role of CIS	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	[redacted]
CC7	Consumer Flag	A flag to indicate whether or not this credit agreements falls under the Consumer Credit Act 1995.	M	[redacted]
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 specific credit card number must return always the same code.	M	[redacted]
CC9	Product Type	Product Type: Credit Card, Credit Card - Shared Limited, Charge Card	M	[redacted]
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	[redacted]
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	NM	[redacted]

		Party, Previous Negative status rectified etc.		[redacted]
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	[redacted]
CC13	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	[redacted]
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	[redacted]
CC15	Contract Request Date	Request Date of the Contract	D	[redacted]
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	[redacted]
CC17	Contract End Actual Date	The actual end date will reflect the date on which the credit card was repaid and account closed.	D	[redacted]
CC18	Payment Made Date	The date on which the last payment was made by the CIS.	NM	[redacted]
CC19	Restructure Event	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	[redacted]
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-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	NM	[redacted]

		relationship between the two accounts)		[redacted]
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	[redacted]
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	[redacted]
CC23	Financed Amount	Total amount of credit that me be drawn or utilised as set out on the credit agreement	M	[redacted]
CI24	MOF Link Code	Multi Option Facility Link is a code which links the sub facilities of a Multi Option Facility **(As this could be a very similar to the provider contract number, an alternative id to be provided to CBI)**	M	[redacted]
CC25	Payment Frequency	Payment Periodicity. Values will include bullet, weekly, fortnightly, monthly, quarterly, annually, etc.	D	[redacted]
CC26	Payment Method	Method of Payment. Values will include cash, direct debit etc.	NM	[redacted]
CC27	Payment Made	The total amount repaid since the last reporting date	NM	[redacted]
CC28	Next Payment Date	The date on which the next payment is due.	NM	[redacted]

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	[redacted]
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	[redacted]
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 down to the nearest whole number	D	[redacted]
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	[redacted]
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	NM	[redacted]

		internal risk management and decision processes of the institution"		[redacted]
CC34	Charged Amount	The amount charged on the Card at the date of reporting and should reflect the total amount of debits as shown on the credit card statement. It is applicable both for Credit Cards and Charge Cards.	NM	[redacted]
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	[redacted]
CC37	Min Payment Indicator	This indicator is used in order to report if the payment was lower than the minimum (0), exactly the minimum (1), or above the minimum payment (2). It is only applicable only when reporting Credit Cards with minimum payments.	NM	[redacted]
CC38	Min Payment Percentage	The percentage of the minimum payment agreed with the CIS is reported here. It is applicable to Credit Cards with minimum payments. A grace period should not be applied to the reporting of this field. For Charge Cards (payable in full each month) the % can be set to 100%.	NM	[redacted]
Body for Record Type: Footer - The last row (and only the last row) will ALWAYS be the Footer.				
FT 1	Record Type	**FT**	M	[redacted]
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	[redacted]
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	[redacted]

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	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

APPENDIX IV: GDPR DATA PROTECTION PRINCIPLES

1. **Lawfulness, fairness and transparency:** Personal data shall be processed lawfully, fairly and in a transparent manner.

    - Has a lawful basis for the processing activity been identified?
    - Is the processing listed in the Record of Processing Activities?
    - Does the processing seem fair, i.e. not excessive?
    - Are we being transparent about the processing? Has the type of processing been identified in the data protection notice or has the data subject been otherwise informed?

2. **Purpose limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes.

    - Will this new project/processing activity involve data being processed in a manner for which it was not collected?
    - Have we been transparent about any extra processes? Is the processing still lawful?

3. **Data minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

    - Are we excessively collecting or processing data?
    - Is the system processing data for purposes other than the purpose for which it was established?
    - Is the data being processed relevant to the purpose?

4. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

    - Are there measures which guarantee the accuracy and correctness of the personal data processed within the information system?
    - Can data be updated, where required?
    - How often is data updated? Is this frequently enough?

5. **Storage Limitation:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

    - Does the system allow data to be deleted when it is no longer required?
    - What retention periods are being implemented? Has a clear justification for these retention periods been established?
    - If data is anonymised/pseudo-anonymised, are we sure that a person cannot be identified using the retained data?

6. **Integrity and Confidentiality:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

    - Have appropriate security controls been implemented to protect the data?
    - Has the IT team been consulted on the effectiveness of the controls in place? Are they in line with ISO27001 or another information security standard?
    - Are the controls which have been implemented proportionate to the nature of the data?

7. **Accountability:** The responsible entities also known as "controllers" take measures to implement programs to eliminate or mitigate data protection 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.

    - Are any risks identified being monitored effectively?
    - Can any decisions made be justified and are documented should an audit take place?

8. **Rights of Individuals:** Citizens and consumers have the right request for access, rectification, portability, or erasure 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.

    - Does the system impose restrictions on the ability to comply with valid subject right requests?

9. **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 data protection.

    - Have appropriate safeguards been established for any transfers of data outside the EU/EEA? (e.g. adequacy agreement or standard contractual clauses)

APPENDIX V: UNIVERSAL DATA PROTECTION 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 realisation 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 organisation can result in changing the use of the data in a completely different way than was ever intended when the database was first constructed.

Unauthorised Use of Unique Identifying Data

Organisations, 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 stigmatised 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.

Unauthorised Processing of Personal Data outside the EU

Transfer of personal data to countries outside the EU and EEA to countries without adequate data 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 unauthorised individuals and can result in unlawful processing.

Large databases are susceptible to data leaks and unauthorised 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 Data protection Risks

Examples of other data protection 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;

- **Stigmatisation** 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 data protection principles. Security and transparency is undermined and a significant accumulation and combination of data can be realised, thereby creating non-transparent and hidden hotspots. Additionally, intelligence services can deploy malware which sabotages security and services providers may be compromised.

APPENDIX VI: RELEVANT LEGISLATION, REGULATIONS AND REFERENCE MATERIAL

Irish Legislation and Regulations

- Credit Reporting Act, 2013 (No. 45)
- Data Protection Acts 1988 – 2018
- European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011; S.I. No. 336 of 2011

European Legislation and Regulations:

- EU General Data Protection Regulation 2016/679