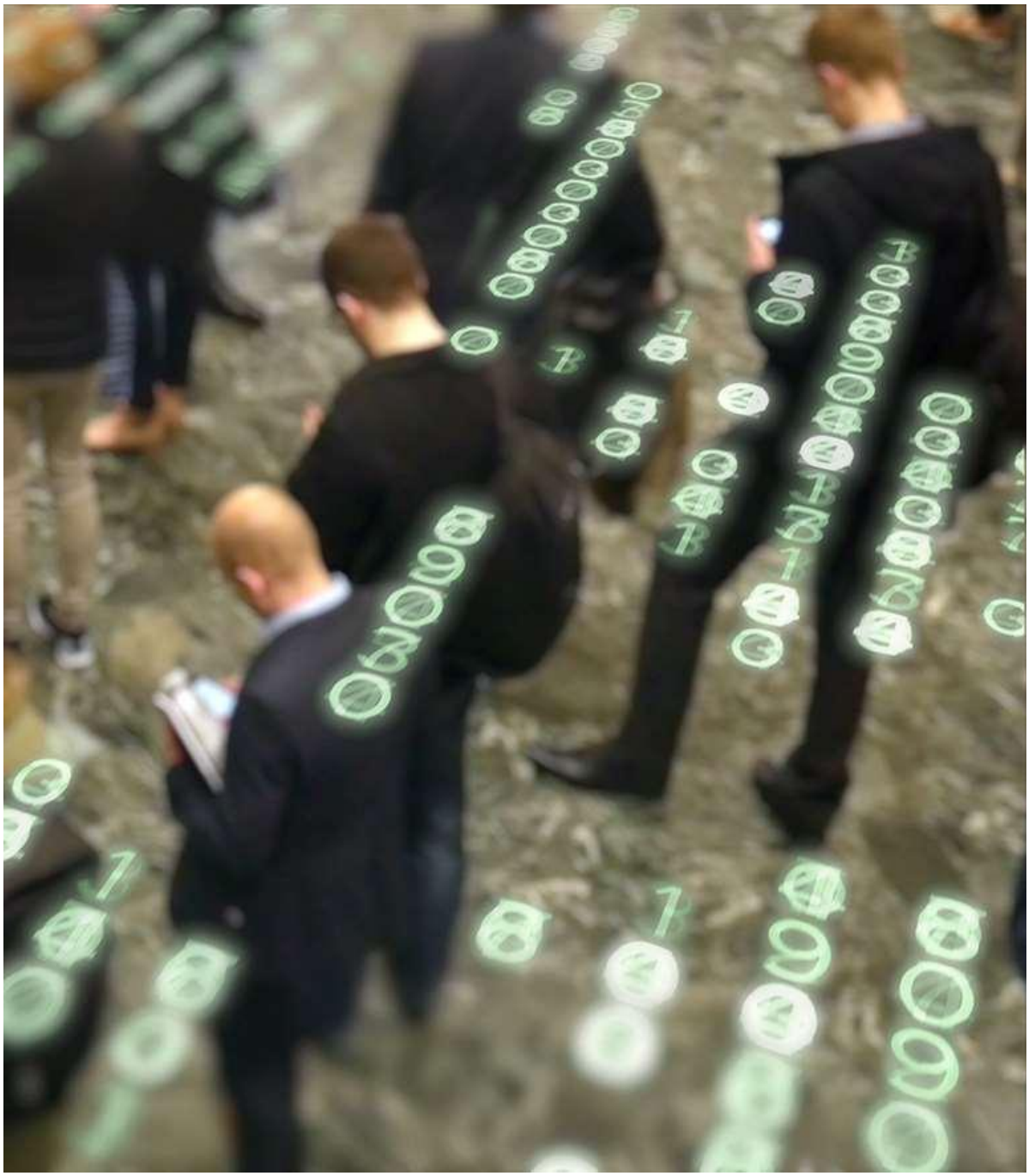
Summary Report: Privacy Impact Assessment - Central Credit Register

May 2018

Version 1.0



CENTRAL CREDIT REGISTER PRIVACY IMPACT ASSESSMENT (PIA) - SUMMARY REPORT

INTRODUCTION

This Privacy Impact Assessment ("PIA") summary report was prepared for the Central Bank of Ireland (CBI") for the purpose of assessing the privacy impact that the introduction of the Central Credit Register ("CCR") will have on individual Credit Information Subjects ("CISs") and assist in the evaluation of potential solutions to those risks.

The PIA was conducted by Mazars, a professional services firm that specialises in providing independent privacy consultancy services including the review of practices for handling personal data.

Mazars reviewed the processes associated with the collection, management and security of CIS-related data including the roles and responsibilities Credit Information Providers ("CIPs") play in the process.

Upon conclusion of the PIA, the CBI addressed identified risks via tailored remediation plans.

CBI is registered as a Data Controller with the Office of the Data Protection Commissioner ("DPC") (reference number: 0397/A).

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 centralization of financial information on borrowers. The legal framework was subsequently established through the Credit Reporting Act 2013 ("the Act").

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

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

The CBI and CIPs will separately perform Data Controller roles, with each being responsible for the data processed within its environments. The CBI will take on the responsibility of Data Controller for the data stored in the CCR and, as part of this role, must ensure that the data protection rights of individuals are upheld. The CIPs will also take on the responsibility of Data Controller for the data that they provide to the CCR. Their obligations to the CISs under the Data Protection Acts[1] do not change under the Credit Reporting Act.

CRIF Ireland Limited will operate the CCR and be a Data Processor on behalf of the CBI, and the CBI will be responsible for ensuring that data is processed in line with the obligations outlined in the Data Protection Act and Credit Reporting Act. CRIF was selected by CBI to be the operator of the CCR following a public procurement process.

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

Figure 1 below outlines the high-level process flow of credit and personal information to and from the CCR,

High Level Data Flow Overview

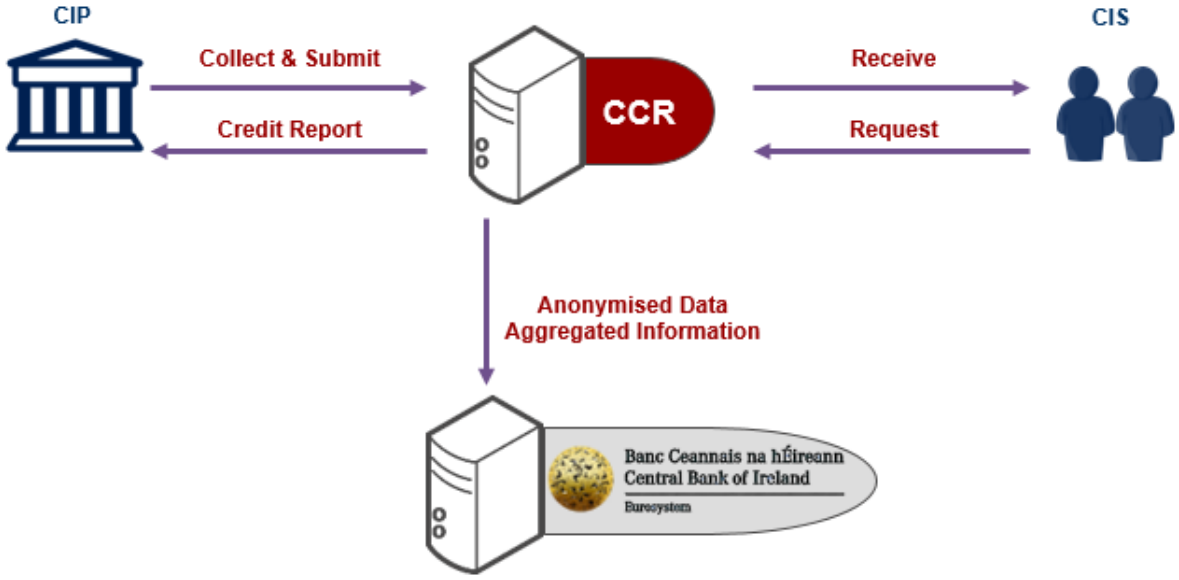


Figure 1: CCR process

THIS DOCUMENT

This report has been prepared by Mazars for the purpose of providing a summary of the PIA. This summary does not disclose all details on the risks identified or remediation actions taken.

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

WHAT IS A PRIVACY IMPACT ASSESSMENT?

A Privacy Impact Assessment (PIA) is a process of systematically considering the potential impact a project or proposed change will have on the privacy of individuals. By completing a PIA, it is possible to not only identify potential privacy issues at the outset of a project but also to design more effective processes for processing personal data and introduce efficient privacy enhancing operations upon completion of the project.

The Mazars PIA methodology uses a standard set of 11 privacy principles. These principles are consistent with the Organisation for Economic Co-operation and Development (OECD), European Union (EU) and national legislation, including the Irish Data Protection Act and the General Data Protection regulation (GDPR), and reflect available best practice guidelines.

WHY IS A PIA IMPORTANT?

A PIA helps organisations identify the risks or potential risks to individuals' privacy that may result from new projects, the introduction of new technology, processes or processing activities. It assists in the evaluation of potential solutions to those risks and sets out recommendations design privacy into the proposed solutions.

WHAT DID THE PIA CONCLUDE?

The PIA identified nineteen privacy risks within the early phase of project design. These risks were reported to the CCR Project for consideration.

WHAT DID CBI DO ABOUT THESE PRIVACY RISKS?

The CBI and CCR Project considered the recommendations of the PIA. Remediation actions to address each of the risks identified (see table below) were implemented by the CCR Project.

#	Privacy Risk	Status as of March 2018
1.	**Fraud** There is a risk that the State could be defrauded through the unauthorised disclosure and use of a PPSN to claim social welfare benefits or tax credits they are not entitled to.	**Closed**
2.	**Snooping** There is a risk that the PPSN could be used by private investigators or others for investigations into a CIS. The risk exists that the PPSN could be sourced from a CIP or the CCR directly	**Closed**
3.	**Unnecessary Over-Transmission of Data** Each month the full submission of all personal data from CIPs to CCR occurs. This submission file, contains both personal and facility data. The transmission of the full Submission data set (e.g. including gender and PPSN) each month represents an overuse of the identifier data contained within the data set.	**Closed**
4.	**Unrestricted Use by CBI** Section 15 of the Credit Reporting Act appears to grant CBI the legal right to use the information stored in the CCR for any of its functions. This creates the risk that CBI uses the data for purposes other than those intended.	**Closed**
5.	**Opportunity for Profiling of Individuals by CIPs** If the CCR mandates CIPs capture PPSN, this will result in PPSN being captured on all borrowers (€500 and over) in the state. A CIP could then use the PPSN to profile individual CISs within an institution using the PPSN as a unique identifier.	**Closed**
6.	**Increased Profiling of Individuals by Government Agencies or State Bodies** Where the PPSN is used in the CCR database it could potentially be used to profile individuals' interactions and behaviour with other agencies or bodies, e.g. Revenue Commissioners, Social Welfare etc. However, at time of writing there is no legislation in place that would allow sharing of the CCR data with other state bodies or agencies.	**Closed**
7.	**CIP Enquiry when Credit Decision is Already Made** As per the Credit Reporting Act, every application for credit over €2,000 requires an enquiry to the CCR. Where the CIS will not be granted credit under the CIPs credit policy there is still an obligation on the CIP to enquire to the CCR. Such an enquiry, when a CIP decision not to grant credit is already made is not consistent with using the data for the purpose it was provided.	**Closed**

#	Privacy Risk	Status as of March 2018
8.	**Quantity of Data Returned** The Credit Reports returned from an enquiry to the CCR will include both personal and facility data relating to a CIS. Only the data that is required to confirm the identity of the CIS and present a clear level of indebtedness and repayment behaviour should be returned. For example where the CIS does not provide a phone number to the CIP, the CCR should not provide phone numbers of the CIS to the CIP.	**Closed**
9.	**Speed of Rectification** The Credit Reporting legislation is compliant with existing Data Protection law to ensure that an error rectification process is in place and that inaccurate data is updated within a defined period of time of 40 days. However, given financial lending decisions, which impact individuals, will be made based on this information, this may be considered too long a time period.	**Closed**
10.	**Abuse of access rights to CCR** There is a risk that CIP employees could abuse access to the CCR by accessing CCR data for purposes other than evaluating a credit application	**Closed**
11.	**Absence of Submission File Encryption** The channel through which the data is submitted to the CCR from the CIP is encrypted. However, the initial design of the submission process does not include file encryption. Given the sensitivity of the submission file, which contains both personal and facility data relating to a CIS, the impact of a security breach to a CIS is potentially very high. As such reliance on tunnel encryption only may not be appropriate	**Closed**
12.	**Unauthorised Access to the CCR** The CCR enquiry service will be available to all internet connected users. As a result, there is a risk of unauthorised access to the CCR via Web access.	**Closed**
13.	**Saving Data to Uncontrolled Systems** As a CIP employee has the ability to download a PDF copy of a credit report via the web portal, there is a risk of a CIP saving credit reports to uncontrolled systems such as home PCs.	**Closed**
14.	**CCR Internal Security** The CCR will result in the creation of several new data stores of personal data. • CDMS (Customer Data Management System) • CIS emails and backups • Core CCR database There will be a reliance on technical security of the CCR to manage the risk to the security of these data hotspots.	**Closed**
15.	**Management of Data Subject Access Requests** There is a risk that an additional personal data hotspot is created within the CBI due to the management of data subject access requests (DSARs) made by a CIS for their data stored both within CBI and the CCR.	**Closed**

#	Privacy Risk	Status as of March 2018
16.	**Sensitive Data Stored by Third Parties** CISs may make credit applications to CIPs through third parties. Where this takes place, there is a risk that the third parties may store or retain the credit application containing CIS personal data, including PPSN, after the application is submitted to the CIP. This risk is increased where the third parties are unregulated entities (e.g. car dealerships) as the CBI does not have a direct or indirect role in regulating these businesses and cannot mandate controls or behaviour.	**Closed**
17.	**Transparency of Use of Data** There is a risk that CISs may not be made aware of all of the purposes their data is being used for or the full breadth of data being sent to the CCR. This is especially true where the uses of the data by the CBI changes over time.	**Closed**
18.	**Notification of Existing Loans Submitted to CCR** There is a risk that the CISs will not be adequately or appropriately notified of the inclusion of existing loans by their CIPs to the CCR.	**Closed**
19.	**Absence of CIS Consent for Data Processing** The Credit Reporting Act gives the CBI the legislative power to process data without an individual's consent. While an individual could, theoretically, choose not to apply for credit and so avoid sharing their data with the CCR, this is not true for existing loans where the applicant which will be included in the CCR database.	**Closed**

REMEDIATION ACTIONS REVIEW

A desk based review of actions taken by CBI to mitigate against risks outlined above was carried out in June 2017 with a follow up in March 2018. The conclusions of the review (i.e. that all the items were closed) was based on conversations with management, copies of reports / guidance documentation.