CENTRAL CREDIT REGISTER PHASE 2 DATA PROTECTION IMPACT ASSESSMENT (DPIA) - SUMMARY REPORT

INTRODUCTION

This Data Protection Impact Assessment ("DPIA") summary report was prepared for the Central Bank of Ireland (CBI") to communicate the data protection and privacy risks to Data Subjects (Credit Information Subjects ("CISs")) resulting from the introduction of the Central Credit Register ("CCR") Phase 2.

Upon conclusion of the DPIA, the CBI addressed identified risks via tailored remediation actions.

BACKGROUND

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 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 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 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 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.

What is a DPIA?

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. Article 35 of the GDPR, as well as Directive (EU) 2016/680, formalises the process for the completion of a DPIA, which 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 Acts, 1988 – 2018, EU General Data Protection Regulation

The Mazars DPIA methodology captures data protection and privacy risks under each of the seven data protection principles as outlined in the GDPR.

Why is a DPIA important?

A DPIA helps organisations identify the data protection and privacy risks or potential risks that may result from new projects, the introduction of new technology, processes or processing activities. 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.

CCR Phase 1 PIA

A Privacy Impact Assessment ("PIA") was conducted for Phase 1 of the CCR. 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 were based on conversations with management, copies of reports / guidance documentation. All items were closed on completion of the follow up testing.

CCR Phase 2 DPIA Scope

Phase 2 of the CCR was not materially different from a data protection and privacy perspective, 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 were being introduced, the conclusions of the Phase 1 PIA did not appear to be materially impacted. There was no significant additional personal data being processed that wasn't considered as part of Phase 1.

However, the inclusion of a data interface from the CCR to the CBI to facilitate a feed of pseudonymised data into a data warehouse 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 scope of the Phase 2 DPIA was the transfer of the pseudonymised from the CCR to the CBI.

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.

High Level Data Flows

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

High Level Data Flow Overview

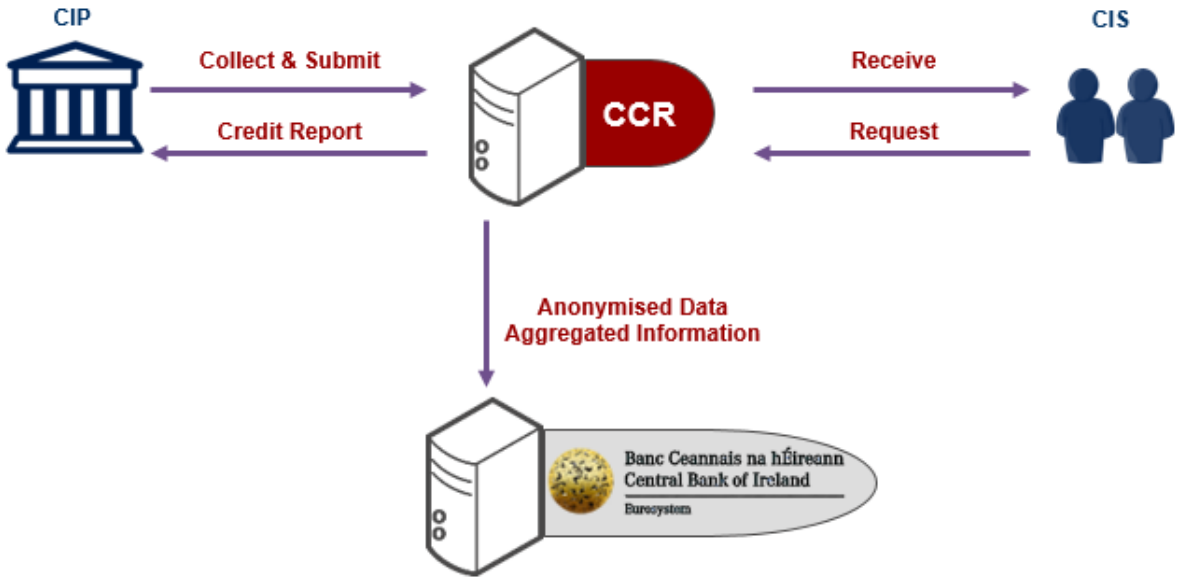

Figure 1: CCR process

MAZARS' DPIA

This report has been prepared by Mazars for the purpose of providing a summary of the DPIA. 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 DID THE DPIA CONCLUDE?

The Phase 2 DPIA identified nine data protection and privacy risks. These risks were reported to the CBI for consideration.

WHAT DID CBI DO ABOUT THESE PRIVACY RISKS?

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

#	Data Protection Risk	Status as of April 2019
1.	**Transparency of Use of Data** 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.	**Closed**
2.	**Purposes for processing data undefined** As CBI functions have not yet defined the uses of CCR sourced data, it cannot be transparently communicated to the CISs the intended uses by the CBI.	**Closed**

#	Data Protection Risk	Status as of April 2019
	CBI functions may have access to pseudonymised data in order to assess what opportunities/potential uses of data. Data may never be used while the access may still be permitted.	
3.	**Sharing data with Government Agencies or State Bodies** Other government agencies / state bodies may request access to the CCR data. While the CBI will adhere to the guidelines issued by the DPC 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.	**Closed**
4.	**Each CBI function requires different subsets of the CCR data set** When a CBI function accesses pseudonymised data held by CBI, the data available is the same for all functions/users. However, each function requires different subsets of the CCR dataset	**Closed**
5.	**Combining CBI datasets** There is a risk that pseudonymised data held by the CBI will be combined with current datasets to identify data subjects	**Closed**
6.	**Retaining information beyond the periods for which it may be held on the Register** CBI will continue to use pseudonymised data obtained from the Register beyond the retention period outlined in the Act.	**Closed**
7.	**Each CBI function will have different retention requirements** There is a risk that every function which requests access to pseudonymised data from the CCR will have access indefinitely, even if the purpose for access/processing will only require one-off access, i.e. there won't be a requirement to compare data over time	**Closed**
8.	**Use the data for malicious intent** Given the scale of data made available to CBI staff, there's an increased risk that data will be used for malicious intent.	**Closed**
9.	**Greater risk of external unauthorised access** Due to the nature of the data being sourced from the CCR and now stored in CBI, there is a risk that it will appealing to potential hackers.	**Closed**

REMEDIATION ACTIONS REVIEW

A desk-based review of actions taken by CBI to mitigate against risks outlined above was carried out in December 2018 with a follow up in April 2019. The conclusions of the review (i.e. that all the items were closed) was based on conversations with management, copies of reports / guidance documentation.