CRIMINAL ASSETS BUREAU

DATA PROTECTION POLICY

Introduction

The Data Protection Act 2018 (hereinafter referred to as "the Act") came into effect on 25 May 2018. The Act amends the Data Protection Acts 1988 and 2003 and gives effect to the Police &Criminal Justice Data Protection Directive (EU) 2016/680 (LED) which applies to the Criminal Assets Bureau (CAB), the Garda Síochána and others in the criminal justice system. The Act also gives effect to the General Data Protection Regulation (EU) 2016/679 (GDPR) which applies to the processing of personal data for purposes other than law enforcement.

The Act is designed to safeguard people's privacy and confers rights on individuals in relation to the privacy of their personal data, as well as responsibilities on individuals and/or organisations holding and processing that data.

As a processor of personal data, CAB has a number of obligations under the Act. This document details CAB's obligations in relation to the privacy rights of individuals and the safeguarding of personal data and the manner in which they are complied with. This document describes how CAB collects, maintains, discloses, uses and destroys personal data.

Role of the Criminal Assets Bureau

CAB is an independent statutory body, established on the 15th of October 1996 pursuant to sections 2 and 3 of the Criminal Assets Bureau Act 1996. CAB is a law enforcement body and as such, is a key component of the criminal justice framework in the State tasked, in particular, with disincentivising criminal conduct, in particular, serious and organised criminal conduct through depriving persons of their ill-gotten gains and disrupting the resources available to support criminal activity.

The objectives of CAB are set out at Section 4 of the Criminal Assets Bureau Act 1996 as follows;

> (a) the identification of the assets, wherever situated, of persons which derive or are suspected to derive, directly or indirectly, from criminal conduct,
>
> (b) the taking of appropriate action under the law to deprive or to deny those persons of the assets or the benefit of such assets, in whole or in part, as may be appropriate, and
>
> (c) the pursuit of any investigation or the doing of any other preparatory work in relation to any proceedings arising from the objectives mentioned in paragraphs (a) and (b).

The functions of CAB are set out at Section 5 of the Criminal Assets Bureau Act 1996 as follows;

> (1) Without prejudice to the generality of section 4, the functions of the Bureau, operating through its bureau officers, shall be the taking of all necessary actions —
>
> (a) in accordance with Garda functions, for the purposes of, the confiscation, restraint of use, freezing, preservation or seizure of assets identified as deriving, or suspected to derive, directly or indirectly, from criminal conduct,
>
> (b) under the Revenue Acts or any provision of any other enactment, whether passed before or after the passing of this Act, which relates to revenue, to ensure that the proceeds of criminal conduct or suspected criminal conduct are subjected to tax and that the Revenue Acts, where appropriate, are fully applied in relation to such proceeds or activities, as the case may be,
>
> (c) under the Social Welfare Acts for the investigation and determination, as appropriate, of any claim for or in respect of benefit (within the meaning of section 204 of the Social Welfare (Consolidation) Act, 1993) by any person engaged in criminal conduct, and
>
> (d) at the request of the Minister for Social Welfare, to investigate and determine, as appropriate, any claim for or in respect of a benefit, within the meaning of section 204 of the Social Welfare (Consolidation) Act, 1993, where the Minister for Social Welfare certifies that there are reasonable grounds for believing that, in the case of a particular investigation, officers of the Minister for Social Welfare may be subject to threats or other forms of intimidation,

and such actions include, where appropriate, subject to any international agreement, cooperation with any police force, or any authority, being a tax authority, being an authority with functions related to the recovery of proceeds of crime, a tax authority or social security authority, of a territory or state other than the State.

In fulfilling our statutory functions, including administration, staffing and resourcing, CAB is required to process personal data within the meaning of the LED, GDPR and the Data Protection Acts 1988 to 2018.

Data Protection Act 2018

The Act came into effect on 25 May 2018 and amends the Data Protection Acts 1988 and 2003 and gives effect to the LED which relates to the protection of individuals with regard to the processing of their personal data by CAB and other competent authorities in the criminal justice system for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of that data.

The LED is a Directive rather than a Regulation, as such, it requires transposition into Irish domestic law to take effect. This transposition is achieved, for the most part through Part 5 of the Act – 'Processing of Personal Data for Law Enforcement Purposes'. The Data Protection Commission (DPC) is set out in Part 5 of the Act as the 'independent supervisory authority' for the LED. Complaints regarding contraventions of the LED regime can be made to the DPC.

The Act also gives effect to the GDPR, which applies to the processing of personal data for purposes other than law enforcement.

Definitions of Key Terms

Terms used in the Act have particular meaning. The following definitions provided by the DPC will assist users of this policy document

Competent authority means a public authority, or other body or entity authorised by law, competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security.

Controllers are those who, either alone or with others, control the contents and use of personal data. Controllers can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as GPs, pharmacists or sole traders. When processing for law enforcement purposes, a controller means a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, or, where the purposes and means of the processing are determined by law, a controller nominated by that law.

Data means information in a form which can be processed. It includes both automated data and manual data.

Automated data means, broadly speaking, any information on a computer, or information recorded with the intention of putting it on a computer.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This can be a very wide definition depending on the circumstances.

Data subject is an individual who is the subject of personal data.

Data processor is a person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment.

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data;
- collecting, organising, storing, altering or adapting the data;
- retrieving, consulting or using the data;
- disclosing the information or data by transmitting, disseminating or otherwise making it available;
- aligning, combining, blocking, erasing or destroying the data.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

Special category personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership. Data subjects have additional rights in relation to the processing of any such data.

In accordance with the provisions of the Act, CAB is a data controller and therefore determines the purpose of the personal data it obtains and how it will be processed.

Principles of Data Protection

The LED and GDPR contain various principles related to the processing of personal data, Article 4 of the LED and Article 5 of the GDPR in particular set out six key principles, which CAB need to be aware of and comply with when collecting and otherwise processing personal data:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality.

CAB as a Data Controller

CAB is the data controller for all personal data processed by its officers and staff. As a data controller, CAB is obliged to implement appropriate technical and organisational measures to ensure compliance with all data protection requirements of the Act. CAB regularly reviews these measures as part of our governance process. This means that the Office adheres to each of the key principles of data protection listed above.

Data Processed on Behalf of CAB

All data processors engaged by CAB must provide sufficient guarantees to implement appropriate technical and organisational measures to comply with the Act and to protect data subject rights. When engaging the services of data processors to process data on our behalf, CAB will enter into a legally binding data processing contract to ensure both our obligations and those of our data processors under the Act are satisfied.

The Act prescribes a number of details and provisions which must be included in data processing contracts. The contract must contain the following details:

- The subject matter, duration, nature and purpose of the personal data processing;
- The type of personal data being processed;
- The categories of data subjects whose personal data is being processed; and
- The obligations and rights of the data controller.

A Data Processing Contract must also include a range of mandatory provisions e.g. documented instruction, confidentiality, security, pre-authorisation of subcontractors, co-operation with data subject requests and audits.

Personal Data Processed by CAB

In line with our statutory objectives and functions under section 4 and 5 of the Criminal Assets Bureau Act 1996, CAB processes a wide range of personal data. The types of personal data processed by CAB may include names, addresses, date of birth, personal public service numbers, incomes, welfare benefits and financial accounts.

In addition to the above, CAB processes data that falls within the definition of special category personal data in Chapter 2 of Part 5 of the Act. In line with our legal obligations under the Act, any processing of special category data by CAB occurs solely in pursuance of its statutory functions conferred under section 5 of the Criminal Assets Bureau Act 1996.

Categories of Data Subjects

Potentially, any category of data subject may have their personal data lawfully processed by CAB. When processing personal data for law enforcement purposes, CAB make a clear distinction between the data of different categories of persons including:

- Principal subjects of CAB investigations
- Secondary subjects of CAB investigations
- Witnesses and other human intelligence sources
- Bureau Officers and Staff
- Stakeholders e.g. State Solicitors, Counsel, Courts Services, the Tax Appeal Commission and the Social Welfare Appeals Office
- Contractors and Suppliers e.g. building and equipment maintenance
- Visitors and other members of the public.

Disclosures to Third Parties

Disclosure in the context of data protection means the provision of personal data to a third party by any means whether written, verbally or electronically. In the performance CAB's statutory functions, it may be necessary to disclose personal data to law enforcement agencies and other third parties, some of which may be located outside this jurisdiction (e.g. the PSNI, Europol or Interpol).

The disclosure of personal data to third parties must have a lawful basis and be necessary and proportionate for achieving the purpose of the processing. The sharing of personal data, including special category personal data, between competent authorities, is specifically provided for under Section 71(5) of the Act for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Right of Access

Pursuant to Article 15 of the GDPR and section 15 of the Act, data subjects, have the right to access personal data relating to them, which is being processed by CAB. Where a request relates to personal data being processed in a law enforcement context this right is not absolute. In order to safeguard the public interest, the Act provides CAB with the right to refuse access to personal data in a number of circumstances, including:

- to avoid obstructing official or legal inquiries, investigations or procedures;
- to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal offences;
- to protect national security or public security; or
- to protect the rights and freedoms of others.

Access may also be restricted where CAB identifies a potential risk to the physical or mental health of the data subject, should the information held be disclosed. In such circumstances, expert medical advice may be sought to inform the approach to the disclosure.

In circumstances where the aforementioned restrictions do not apply, an individual who believes their personal data is being processed by CAB has a right to:

- a copy of the data being held relating to them;
- be informed as to the purpose and legal basis for the processing;
- know the categories of personal data concerned;
- be told the recipients or categories of recipients to whom their personal data have been disclosed; and,
- where possible, informed of the period for which the personal data will be retained.

Information must also be provided as to the origin of the data concerned, however, the Act allows for restrictions on the information provided in a law enforcement context if such a disclosure would not be in the public interest.

Data subjects may request that inaccuracies in their personal data be corrected or erased. Such requests may not be made in relation to personal data contained in the witness statements of third parties.

If an individual, who believes their personal data is being processed by CAB, wishes to know the above information, they can submit a Subject Access Request to:

Data Protection Officer
Criminal Assets Bureau
Walter Scott House
Military Road
Dublin 8
D08HE2P
Ireland

Or by email: info@cab.ie

Making a Subject Access Request

The Subject Access Request must be submitted by completing the Subject Access Request form, which can be found on the CAB website (www.cab.ie).

All Subject Access Requests must be submitted to the CAB Data Protection Officer at the address listed above. To ensure our Data Protection Officer can verify the identity of applicants and locate their personal data, requests must be accompanied by a copy of the applicant's driver's licence, passport or public services card.

With the exception of the parents/guardians of minors and authorised legal representatives, CAB will only accept Subject Access Requests from the individual concerned.

There is no fee charged for making reasonable requests. Requests deemed to be manifestly unfounded or excessive will be refused. We aim to respond to valid requests within one month from the date the applicant's identity is verified.

Data Protection Impact Assessment (DPIA)

CAB conducts a Data Protection Impact Assessment (DPIA) when engaging in personal data processing activities that may present a high risk to the rights and freedoms of individuals. This process ensures compliance with data protection legislation and promotes transparency in data handling.

DPIA Risk Assessment Process

- A risk assessment will be conducted to determine whether a DPIA is required for a specific data processing activity.
- The assessment will identify potential risks associated with the processing and evaluate whether mitigation measures can sufficiently reduce those risks.
- All identified risks and mitigation strategies must be clearly documented and retained for audit and compliance purposes.

Roles and Responsibilities in Conducting a DPIA

- Data Controllers: Responsible for initiating and conducting the DPIA in coordination with relevant stakeholders.
- Data Processors: Must support CAB by providing necessary information on data processing activities and implementing required security measures.
- DPO: Provides guidance, ensures DPIA documentation is complete, and determines if consultation with the DPC is required.
- Senior Management: Oversees compliance with DPIA findings and ensures that mitigation measures are properly resourced and enforced.

Triggers for Conducting a DPIA

A DPIA must be conducted in any situation where data processing is likely to result in a high risk to individuals. The following constitute high-risk processing activities:

- Systematic and extensive evaluation of personal aspects based on automated processing large-scale processing of sensitive personal data
- Use of new or innovative technology in data processing that impacts data subjects' rights.
- Combining datasets in ways that increase the risks of re-identification or profiling.
- Any data processing that involves cross-border data transfers with potential jurisdictional risks.

Documentation of DPIA

All DPIAs must be documented using the required DPIA template, ensuring a thorough assessment of risks, mitigation strategies, and justifications for processing.

Periodic Review of Existing DPIAs

- Existing DPIAs must be periodically reviewed to ensure that they remain relevant and effective.
- Reviews should occur when there are significant changes in data processing activities, new risks emerge, or legislative changes impact the processing environment.

Maintenance of a DPIA Log

- CAB will maintain a DPIA log, recording all assessments conducted, including dates, findings, and subsequent actions taken.
- The log will be regularly updated and made available for internal and regulatory review.

By implementing these measures, CAB ensures compliance with data protection legislation and upholds the highest standards of data privacy and security.

Personal Data Security Breaches

A ‘personal data breach’ is a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data stored, transmitted or otherwise processed.

Breaches include accidental and deliberate acts, and breaches of personal data done knowingly or recklessly are an offence under the Act. Section 145 of the Act provides for individuals to be liable for prosecution in the event of an unauthorised disclosure of personal data.

CAB has implemented a range of high level security measures designed to prevent unauthorised access to processing equipment or personal data.

All personal data breaches must be reported to the CAB Data Protection Officer immediately. If it is determined that the personal data breach represents a risk to the rights and freedoms of the data subject, the Data Protection Officer will notify the Data Protection Commission within 72 hours. It may be necessary to notify data subjects of any breach of their personal data also in order that they can also take steps to mitigate against the breach.

Oversight by Data Protection Commission

The DPC is the national independent authority responsible for upholding the fundamental rights of individuals to have their personal data protected. The DPC is the competent supervisory authority for handling complaints from data subjects regarding processing of their data, and for investigating incidences of data breaches.

The DPC has the power to conduct inquiries and audits of organisations to assess their compliance with data protection legislation. This includes powers for authorised officers of the DPC to enter premises of the data controller and inspect personal data being held on computer systems or other relevant filing systems. If infringements are found and improvements are required, the DPC has corrective powers.

CAB will make every effort to cooperate and assist the DPC in the performance of its functions on receipt of any request for same.

Complaints

Data subjects are entitled to submit complaints relating to CAB's management of their personal data to the DPC at:

Data Protection Commission
21 Fitzwilliam Square
Dublin 2
D02 RD28
Ireland
www.dataprotection.ie

Related Documentation

This document should be read in conjunction with CAB's Website Privacy Statement, available at www.cab.ie/privacy-policy-cookies/. Our Website Privacy Statement informs visitors to the www.cab.ie website about how we collect and use their information.