Guidance for Individuals who Accidentally Receive Personal data

An Coimisiún um Chosaint Sonraí
Data Protection Commission

The Risk of Accidental Disclosure

Information and communication technology plays an increasingly large role in our working and private lives and has many advantages, including convenience. However growth in the processing and transmission of personal data can also increase risks to privacy. One such risk arises when a data controller (a person, company, or other body which collects and uses personal data) accidentally discloses personal data to another individual.

These incidents are known as personal data breaches and there are many ways they can unfortunately happen:

- A bank accidentally issues statements or other correspondence to the incorrect recipient via post or email;
- A government body accidentally issues correspondence to the wrong recipient or address;
- A clinic mistakenly puts a medical report into the wrong envelope and sends it the wrong patient;
- A business disposes of an old laptop without erasing a disk drive containing HR data;
- A mistyped email address sends confidential financial information to an unconnected third party;
- A USB drive containing customer contact details is left behind on a train.

Mistakes like this can lead to an individual's personal data being disclosed to another individual who had no intention or expectation of receiving it. It is easy to imagine how sensitive that data may be. It is also easy for a person who has accidentally received someone else's personal data to imagine how distressed they might be if their own data was accidentally disclosed to a stranger.

The rights of data subjects – that is, individuals personal data may identify – have special protection under the General Data Protection Regulation (GDPR), the Data Protection Act 2018, the European Convention on Human Rights, the EU's Charter of Fundamental Rights and other laws. An individual who accidentally receives another individual's personal data should recognise and respect those rights.

Dealing with Accidental Disclosure

The Data Protection Commission (DPC) recommends that an individual who accidentally receives personal data that is not their own should act promptly and take steps to reduce the risks to the rights of the individual/s the data relates to:

- Identify the data controller (for example from the sender's email address or letterhead) and inform them of the mistaken disclosure. Do not wait for them to contact you.
- Avoid opening email attachments, files or papers that are not yours to open.
- Agree with the data controller how to resolve the mistake. It may be sufficient to permanently delete an email from your 'inbox' and 'deleted files' folders. The data controller may arrange to collect a misaddressed letter or parcel from you, or you may agree to destroy it, for example by securely shredding the information and confirming in writing to the data controller that you have done this.
- If you cannot identify or contact the data controller, contact the DPC using our webform or email us. We will try to help resolve the problem.
- Do not attempt to identify and contact the person the data belongs to as this is further processing the information.
- Do not share the data with another third party including publically uploading information to social media platforms.

Data Controllers and Unlawful Processing

If a personal data breach results in an individual accidentally receiving another individual's personal data, the individual should not make a bad situation worse. In particular, they should not seek to become a controller of that data, and they must not process the data without a lawful basis for doing so.

As already mentioned, a data controller is a person, company, or other body, which decides the purposes and methods of processing personal data, whether on their own, or jointly with another person/s or organisation. Processing has a wide definition in data protection law. It includes not just computing and analysing data, but also disclosing it, transmitting it, editing or converting it to different formats, and even simply retaining it. It can apply to personal data in hard copy, such as printed documents, as well as to electronic data such as email or computer files.

If an individual who has accidentally received personal data takes it on themselves to decide how that data should be processed they may be deemed a controller in respect of that data. This can have significant legal consequences.

Unlawful retention or other processing of personal data can lead to civil law consequences. Data subjects and the lawful data controller can both seek significant remedies in the courts, which can include injunctions, damages and costs.

The DPC has extensive powers to enforce data protection laws. These include powers to conduct inquiries, to require the production of documents and records, to prohibit unlawful processing and to order the deletion of data. It can impose administrative fines and bring criminal prosecutions for breaches of data protection laws. (Under section 145 of the Data Protection Act 2018, unauthorised disclosure of personal data is a crime that can be punished with a fine of up to €50,000 and/or imprisonment for up to five years.)

The DPC strongly recommends that any individual who accidentally receives personal data that is not their own should respect the rights of the data subject and of the data controller lawfully responsible for the data. They should not seek to hold or use the data unlawfully for their own or any other purpose.