Guidance for Organisations Accidentally in Receipt of Personal Data

An Coimisiún um Chosaint Sonraí
Data Protection Commission

The purposes for which we give and receive personal data increase daily, and the volume of personal data processed and transmitted by individuals and organisations continues to grow. It is increasingly likely that organisations will accidentally come into possession of personal data that they did not expect or intend to deal with. For example:

- An organisation receives a letter or package that has been wrongly addressed because of a mistake in the sender's mail room;
- A customer intending to upload a photo of a defective product accidentally sends their holiday pictures instead;
- Careless use of the auto-fill function when addressing an email causes personal data to be sent to the wrong person;
- A visitor to an office inadvertently leaves behind personal papers or a USB thumb drive.

An organisation, whether in the public, private or voluntary sector, must be aware of the possibility of finding itself accidentally in possession of personal data. The broad definition of 'processing' in Article 4(2) of the GDPR means that opening, transmitting, deleting or simply storing personal data that you have unintentionally acquired will bring the GDPR into play.

An organisation that acquires control over personal data – however innocently or accidently – must deal with it in a way that respects its obligations as a data controller. It may not process that data – whether by reading, transmitting, editing, and storing it – unless one or more of the six legal bases listed in Article 6 of the GDPR applies:

1. **Consent:** the data subject has provided clear consent to your organisation to process their personal data for a *specific* purpose;
2. **Contract:** the processing is necessary to perform a contract that your organisation has with the data subject;
3. **Legal obligation:** the processing is necessary for your organisation to comply with law;
4. **Vital interests:** the processing is necessary to protect the life of an individual;

5. **Public interest:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law;
6. **Legitimate interest:** the processing is necessary for your organisation's legitimate interests or those of a third party, and these outweigh any competing interests of the data subject. (This is not available to public authorities processing data to perform their official tasks.)

If the data belongs to one of the special categories of data listed in Article 9(1) of the GDPR, the legal bases for processing are further restricted. The special categories include personal data relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic or biometric data uniquely identifying a person;
- Health data; and
- Sex life or sexual orientation.

A data controller in possession of special category data should be aware of and take particular care to respect the very high standards of protection set for it in data protection law.

If an organisation finds itself in control of personal data without a legal basis for processing it, it should not make a bad situation worse. Unlawful processing of personal data can and does lead to regulatory action including investigations, administrative sanctions and criminal prosecution. Data subjects can also take civil actions for breach of data protection law.

The Data Protection Commission (DPC) recommends that organisations that come into accidental possession of personal data take immediate steps to identify the rightful data controller and remedy the breach. It should do so in a way that involves the minimum of intrusion or exposure:

- Respond promptly to a misaddressed email informing the sender of their mistake, and permanently delete the copy you received without opening any attachments.
- If possible, identify the sender of a misaddressed letter or package from the postmark, label or letterhead. Do not read through material not intended for you.
- If you retain materials pending retrieval by the lawful controller, keep the data in a secure place where it cannot be mistakenly accessed or removed.

If the rightful data controller cannot be identified or contacted, you can contact the DPC. We will try to assist you in identifying the rightful data controller with a view to remedying the breach.

Once the rightful data controller has been identified, the DPC will advise them of their obligations under Article 33 of the GDPR where appropriate.