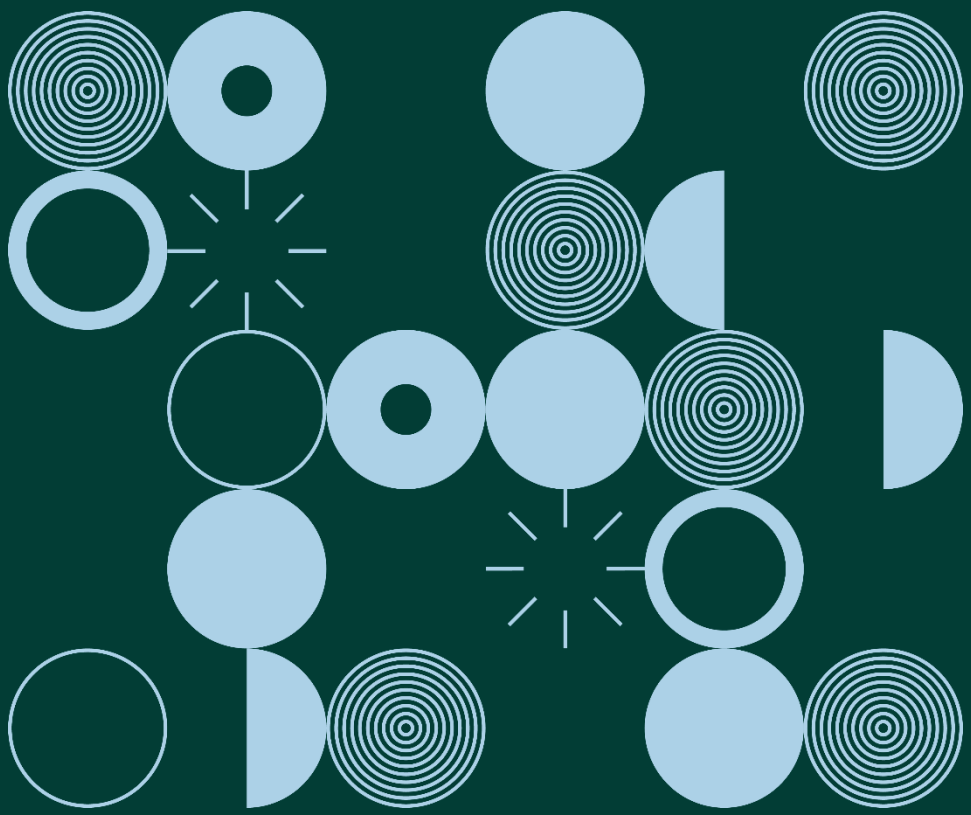
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

Data Security Guidance for Microenterprises

July 2019



Contents

Data Security Guidance for Microenterprises

The General Data Protection Regulation (GDPR) enhanced the obligations and responsibilities of organisations and businesses with regard to how they collect, use, and protect personal data.

At the heart of the GDPR is the requirement for organisations and businesses to be transparent about how they are obtaining, using, and safeguarding personal data. This transparency requirement is outlined under Article 12 GDPR and encompasses the provision of clear, concise information to data subjects and the facilitation of data subjects' rights.

Additionally the principle of accountability, which is outlined under Article 5 GDPR, means that organisations and businesses are responsible for demonstrating their compliance with the GDPR's principles relating to the processing of personal data.

The Data Protection Commission (DPC) has developed this guidance to assist microenterprises in implementing the appropriate technical and organisational security measures to safeguard the personal data they are processing.

A microenterprise is defined as an organisation having fewer than 10 employees and an annual turnover (the amount of money taken in a particular period) or balance sheet (a statement of a company's assets and liabilities) below €2 million.

If your company is a microenterprise engaged in the processing of personal data, as either a data controller or a data processor, you will be subject to the provisions of the GDPR. A data controller is defined under Article 4 GDPR as a natural or legal person that determines, alone or jointly with others, the purposes and means of the processing of personal data. The same Article defines a data processor as a natural or legal person that processes personal data on a data controller's behalf.

The GDPR is applicable to the processing of personal data by microenterprises established in and operating outside the European Union (EU). If your company is established in the EU, the provisions of the GDPR are applicable to your processing of personal data in the context of the activities of your EU establishment(s).

If your company is not established in the EU, the GDPR is applicable to your processing of the personal data of individuals in the EU with regard to the offering of goods or services (regardless of whether payment is involved) and to the monitoring of an individual's behaviour (in so far as that behaviour takes place within the EU).

Microenterprises are also encouraged to read the DPC's more detailed guidance on data security, available on the DPC website, 'Guidance for Controllers on Data Security'.

Know Your Data

Microenterprises should regularly review the personal data they process and determine what personal data and, in particular, what special categories of personal data, they hold.

'Personal data' are defined, under Article 4 GDPR, as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 9 of the GDPR defines **'special categories of personal data'**, as data relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, and data concerning an individual's sex life or sexual orientation.

Principles you must adhere to with regard to the processing of personal data are outlined in Article 5 GDPR. When considering your company's processing, questions to be asked include whether you are processing personal data:

- ✓ according to the principles of lawfulness, fairness, and transparency;
- ✓ for specified, explicit and legitimate purposes;
- ✓ with a view to data minimisation;
- ✓ with a view to ensuring accuracy and, where necessary, that data is kept up to date;
- ✓ such that data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of processing; and
- ✓ in a manner that ensures appropriate security of the personal data.

If you outsource the processing of personal data to a data processor (including, for example, to a 'cloud computing' service provider), you should be able to confirm that:

- ☐ the processing is compliant with Article 28 GDPR;
- ☐ the processor's security procedures are adequate; and
- ☐ you have sought and been given assurances regarding the appropriate security measures from the processor.

Determining the Appropriate Level of ICT Security

Article 32 GDPR obliges data controllers and data processors to implement the technical and organisational measures necessary to ensure an appropriate level of security in relation to the risks presented by processing. In considering what constitutes an appropriate level of security, you should take into account.

- "The state of the art";
- "The cost of implementing and the nature of the scope";
- "The context and purposes of processing"; and

- "The risk of varying likelihood and severity for the rights and freedoms of natural persons".

The following guidance deals with the different types of security microenterprises should consider when assessing what they need to do to ensure their processing of personal data is in compliance with the security and integrity obligations of the GDPR.

Technical Security

Technical security measures protect ICT systems by ensuring that appropriate technology is implemented to secure personal data processing.

Examples of practical technical security measures are:

- ✓ ensuring that all computing devices such as PCs, mobile phones, and tablets are using an up-to-date operating system;
- ✓ ensuring all computing devices are regularly updated with manufacturer's software and security patches;
- ✓ using antivirus software on all devices;
- ✓ implementing a strong firewall;
- ✓ reviewing vendor supplied software and updating default system, administrator, and root passwords and other security parameters to ensure defaults are not left in place;
- ✓ ensuring data backups are taken and are stored securely in a separate location;
- ✓ ensuring that data backups are periodically reviewed and tested to ensure they are functioning correctly;
- ✓ ensuring that data is collected & stored securely;
- ✓ ensuring that mobile devices (such as laptops and mobile phones and tablets) are encrypted;
- ✓ ensuring that two-factor authentication is enabled for remote access;
- ✓ ensuring that websites have TLS (transport layer security) in place to securely collect personal data via webforms (such as for newsletter subscriptions) or on e-commerce websites.

Additional information, advice, and best practice regarding technical security standards can be found at the websites of the European Union Agency for Network and Information Security (ENISA) and the US-based National Institute of Standards and Technology (NIST).

Physical Security

Physical ICT security measures assist organisations with the protection of ICT systems such as facilities, equipment, personnel, resources, and other properties. Examples of ICT equipment that may require protection includes any device which can store information electronically, such as:

- ✓ Computers — servers, desktop, laptop or tablet
- ✓ Photocopiers, multifunction devices and printers

- ✓ Mobile telephones
- ✓ Digital cameras
- ✓ Storage media–for example, portable hard drives, USB sticks, CDs, DVDs

The level of protection that should be applied to ICT equipment is based on the business impact level that may result from data being compromised, loss of integrity, or unavailability of the electronic information held on the device, this would also include the loss or unavailability of the device due to a failure.

Examples of practical physical security measures are:

- ✓ keeping offices and storage units locked;
- ✓ keeping server rooms or cabinets locked;
- ✓ cabling desktop machines and laptops to desks;
- ✓ implementing clean desk policies;
- ✓ ensuring that fire and burglar alarms are in place and that they are functioning correctly;
- ✓ ensuring that ICT equipment such as hard drives and old laptops, computers and mobile devices are securely disposed of at end of life.

Organisations should also assess the risk arising when devices cannot be secured when not in use. Where an organisation has determined the business impact of the data compromise, loss of integrity or unavailability regarding a device, which is not in use, organisations should ensure that such devices are stored securely.

The DPC also recommends that microenterprises design and implement an asset control policy for ICT equipment. This would include:

- ✓ recording the location and user of the device; and
- ✓ conducting periodical audits of its ICT equipment.

Organisational Security

Organisational security measures protect ICT systems by ensuring that policies, procedures, training, and audit trail functions are in place.

These measures are mostly documentary in nature, however such policies need not be time consuming nor overly complicated to implement. Any documentation should be written in clear, concise, language, should list the rules that apply to the processing of personal data, and should be readily accessible to employees. Such documentation should be reviewed periodically to ensure that it is accurate and up-to-date.

Examples of practical organisational security measures consist of:

- ✓ communicating the importance of company data and all the measures they can take to protect it to employees;

- ✓ conducting ongoing staff training on, but not limited to, social engineering attacks, crypto ransomware, and data protection;
- ✓ documenting data collection and retention policies;
- ✓ ensuring the use of strong passwords by having a password policy in place that is enforced;
- ✓ ensuring remote access is supported by a remote access policy;
- ✓ documenting a data breach incident response plan and testing it periodically to ensure a data breach can be effectively responded to;
- ✓ documenting CCTV policies (where appropriate);
- ✓ documenting data back-up policies;
- ✓ periodically reviewing contracts with 3rd party ICT providers to ensure the security measures documented are still appropriate and up to date.

Data Collection and Retention Policies

In all cases, but in particular if your organisation will be holding personal data for longer periods, you should be aware of your obligations under Article 5(1)(e) GDPR, as both a data controller and a data processor with regard to data retention.

Personal data should not be retained in an identifiable form for longer than is necessary in relation to the purposes for which such data is processed. A pragmatic approach to retention is simply to delete the data once the purpose for which it was processed has ceased.

Data collection and retention should be assessed against business needs and minimised, either by not collecting unnecessary data, by deleting data, or by rendering it anonymous. Microenterprises should:

- ✓ Define and implement a data collection policy. The policy should detail the categories of personal data collected and the purposes for collection.
- ✓ Define and implement a data retention policy. This policy should detail the retention period for personal data collected and measures taken to ensure deletion or if applicable, the techniques to render the data non-identifiable.

These policies should be communicated to all employees and periodic reviews should be conducted to ensure that personal data is handled correctly when it is no longer needed for the purposes for which it was collected.

With regard to retention policies, if you intend to further process personal data for the purposes of archiving, scientific or historical research, or statistical purposes, you should ensure appropriate safeguards are in place to ensure the rights and this processing does not impede freedoms of data subjects.

In particular, these safeguards should ensure that technical and organisational measures are in place to ensure respect for the principle of data minimisation.

A documented retention policy should offer guidance and provide a framework for employees to manage information across its lifecycle so that your company complies with the laws and regulations pertaining to data management. A retention policy should apply to both physical and digital formats.

Utilising Data Processors

Microenterprises, due to a lack of in-house expertise, may rely on third party data processors to process personal data on their behalf, such as e-commerce websites, cloud services such as email or online data backup solutions. Microenterprises should:

- ✓ Define the responsibilities of the data controller and data processor and ensure that processing is carried out on foot of a written agreement detailing the appropriate technical security and organisational measures to be applied by the data processor specifically in relation to the personal data processing operations.
- ✓ Obtain sufficient guarantees regarding the security measures applied by processors acting on their behalf and periodically review to ensure that the terms of the written agreement are being adhered to.

A practical way for a microenterprise to obtain sufficient guarantees and ensure compliance is to:

- ✓ Use a data processor that has vendor certification, appropriate IT qualifications and/or certification, or the appropriate certification from a relevant certifying body such as the International Organization for Standardization or the Payment Card Industry.
- ✓ Have formal project completion / change management sign off procedures in place to ensure that appropriate security measures are implemented and that changes/updates are performed.
- ✓ Have data processors provide regular reports on the management of the ICT systems and following up to ensure that work is carried out.
- ✓ Review security measures periodically to ensure they are up to date, this can be especially prevalent when utilising Cloud-Based environments. The DPC published guidance for organisations utilising Cloud Based environments which sets out further steps how an organisation can review its security measures.

Five Steps to Secure Cloud-Based Environments

Cloud-Based environments offer many advantages to organisations. However, they also introduce a number of technical security risks which organisations should be aware of such as:

- ✓ Data breaches
- ✓ Hijacking of accounts
- ✓ Unauthorised access to personal data

Organisations should determine and implement a documented policy and apply the appropriate technical security and organisational measures to secure their cloud-based

environments. If organisations do not implement such controls, they may increase their risk of a personal data breach.

Organisations should apply technical security and organisational security measures in a layered manner consisting of but not limited to:

- ✓ Access controls
- ✓ Firewalls
- ✓ Antivirus software
- ✓ Staff training
- ✓ Policy development

A layered approach to cloud-based security mitigates the risk of a single security measure failing which may result in a personal data breach.

Many cloud-based providers, such as Microsoft's Office 365 and Google's G-suite provide advanced settings and solutions which can assist organisations to appropriately secure their use of cloud-based services. These providers, in most cases, also offer best practice guidance to assist organisations in securing their cloud-based environments.

Additional information, advice, and best practice regarding technical security standards for cloud-based environments can be found at the websites of the European Union Agency for Network and Information Security (ENISA) and the US-based National Institute of Standards and Technology (NIST).

The DPC has listed five key ways organisations can secure their cloud-based environments to mitigate their risk of a personal data breach.

- ☐ Organisations should implement strong password polices to ensure that users accessing personal data within cloud-based environments do so in a secure manner.
- ☐ Organisations should implement two-factor authentication. Two-factor authentication is an effective way to further enhance cloud-based security and is available from most cloud-based providers.
- ☐ Organisations should be aware of and document user access privileges within their cloud-based environments. User access control is particularly important where group mailboxes or shared folders are utilised. Organisations should also document each user's specific access requirements and ensure that these are supported by an appropriate change control process.
- ☐ Security measures applied by an organisation must be supported by regular reviews of user access to ensure that all authorised access to personal data is strictly necessary and justifiable for the performance of a specific function.
- ☐ Organisations should not rely on cloud-based service providers' default security settings.

Organisations should review the cloud-based security features available from the cloud-based service provider to ensure that they are applied appropriately and in a layered manner. Examples of security settings and controls provided by cloud-based service providers often include:

- ✓ Centralised administration tools
- ✓ Mobile device management
- ✓ Multifactor authentication
- ✓ Login alerts
- ✓ Encryption during message send and receive
- ✓ Encryption of message content
- ✓ Account activity monitoring and alerts
- ✓ Data loss prevention
- ✓ Malware protection
- ✓ Spam and spoofing protection
- ✓ Phishing protection

Organisations should also be aware that cloud-based services might be publically accessible and organisations should review and implement the appropriate security settings to secure remote access.

Assurance from ICT Service Providers

Organisations may utilise external ICT services providers to implement their cloud-based environments. It is vital during such engagements that organisations seek formal assurances from their ICT service provider that the security controls which have been implemented meet an organisation's specific security requirements and protect the organisation's personal data.

Organisations should proactively engage and conduct regular security reviews with their ICT service providers to ensure the security controls in place are up-to-date and are effective to protect the organisation in an evolving threat landscape.

Clear Policies and Staff Training

Organisations should ensure that staff receive appropriate training on social engineering attacks, phishing attacks and security threat practices. Such training should be supported by refresher training/awareness programmes to mitigate the risk posed by an evolving threat landscape.

Organisations should have clear policies in place with respect to the usage and security of their file storage, network infrastructure, and/or cloud-based services, especially where these services are being accessed outside of the organisation corporate network under Bring Your Own Device (BYOD) policies.

Organisations should have clear "employee leaver" and "succession" policies in place and these should be applied to an organisation's on- and offline file and permission management systems.

Organisations should have a clear policy in place for data retention and conduct regular reviews to ensure that personal data is not retained longer than necessary or where the original purpose for the use of the personal data has ceased.

Know and Secure Your Data

Organisations should understand and monitor the types of personal data that they store or otherwise process. Knowing the types of personal data processed enables an organisation to ensure the appropriate security and access controls are applied to protect the data.

Organisations should utilise data classification methods to identify the data which they store and process. The process of data classification enables an organisation to categorise their stored data in order to determine the appropriate security controls.

Organisations should carefully evaluate any external vendors based on the security features they offer and how they specifically meet with their organisational requirements.

Who has access to your data, how is it secured, how often is the data backed up, and whether external service providers, such as vendors for cloud-based environments, align to your organisational policies, are all vital questions to ask of both your cloud-based service provider and / or the ICT service provider charged with implementing your environment.

Applying the appropriate security measures is not a once off "Set and forget" exercise. Security procedures and settings should be reviewed on a regular basis to ensure that they are still appropriate and up-to-date.