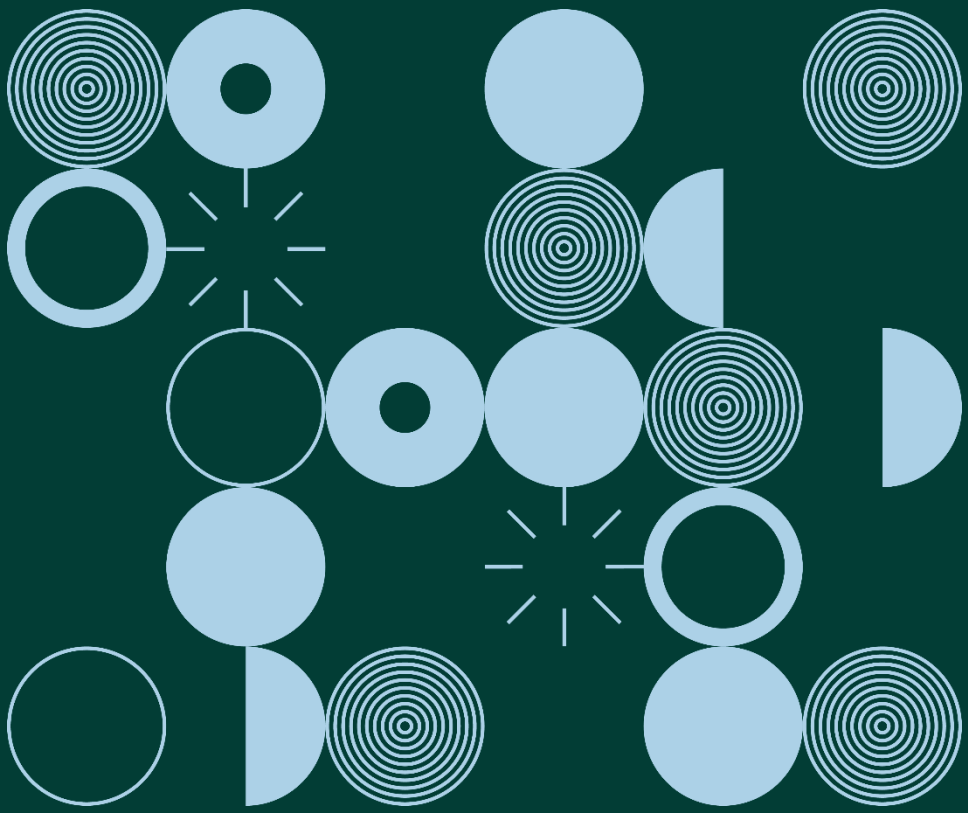
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

Guidance for Controllers on Data Security

February 2020



Contents

Guidance for Controllers on Data Security

Data controllers in the private and public sectors hold increasing amounts of personal data on individuals. The decreasing cost of electronic storage and processing has greatly contributed to this. Organisations also increasingly outsource data processing to third parties to undertake on their behalf (data processors). Many organisations also continue to hold large quantities of personal data in manual form – often in off-site locations.

This large increase in the quantity of personal data processed and held gives rise to security challenges for the organisations that collect the data. Data controllers need to regularly audit their holdings of personal data and the procedures they have in place to protect this data. Questions they should ask include:

- ✓ Do we know what types of personal data we hold:
  - electronically (including less obvious data such as CCTV images)?
  - on paper?
- ✓ Can we justify the collection of this information?
  - Why do we collect it?
  - What it is used for?
  - What are the risks?
  - How long do we hold it?
  - Who has access to it?
  - To whom do we disclose it?
  - Where will the data be stored?
  - Is it held securely?
  - How we dispose of the personal data?
- ✓ If we outsource processing of personal data to a data processor (including a 'cloud computing' service provider), are we satisfied that their security procedures are adequate?

The Law

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) do not detail specific security measures that a data controller or data processor must have in place, though the European Communities (Electronic Communications Networks and Services) (Privacy and Communications) Regulations 2011 ('the ePrivacy Regulations') detail some requirements specific to the electronic communications services sector.

The GDPR, in Articles 25 and 32, does however place an obligation on controllers and processors to implement data protection by design and by default and 'appropriate technical and organisational measures' to ensure a level of security appropriate to the risk, taking into account:

- the state of the art;
- the costs of implementation;
- the nature, scope, context and purposes of processing; and
- the likelihood and severity of the risk to the rights and freedoms of individuals.

It goes on to suggest the following indicative list of appropriate measures;

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effective of technical and organisational measures for ensuring the security of the processing.

Data controllers and data processors are also obliged to ensure that their staff and other persons at the place of work are aware of security measures and comply with them. The legal obligation to keep personal data secure applies to every data controller and data processor, regardless of size.

In this guidance note certain issues are identified that data controllers and processors should consider when developing their security policies.

Data Collection and Retention Policies

The most effective means of mitigating the risk of lost or stolen personal data is not to hold the data in the first place. Data retention and replication should always be assessed against business need and minimised, either by not collecting unnecessary data or by deleting data as soon as the need for it has passed. Holding any personal data presents security risks. An example is organisations manually collecting full credit card details including expiry date and CVV number and storing such information beyond the processing of the transaction.

A data controller should always know what personal data they hold, where they are held and how it flows through the organisation. Without this element of oversight, effective protection of personal data within the organisation is a difficult task.

Data processors are subject to the same security obligations as data controllers. Therefore references to 'data controllers' in this guidance note also cover data processors, unless the context indicates otherwise.

Access Controls

A data controller has a duty to limit access to personal data on a "need to know" basis. Greater access limitations or controls should apply to more sensitive data. A data controller must be aware of the different users who access their systems/records and their requirements. The different types of users could include:

- staff at various seniority, operational or responsibility levels;
- third party contractors/data processors;
- customers; and
- business partners.

Consideration must be given to the different requirements of each of these types of user and their access privileges to personal data should fully reflect these requirements.

The nature of access allowed to an individual user should be set and reviewed on a regular basis. Individual staff members should, among other things, only have access to data which they require in order to perform their duties, prevent use of shared credentials (multiple individuals using a single username and password) and detect use of default passwords. Specific procedures sometimes referred to as a "movers, leavers and joiners" policy are required in all organisations with access to personal data to decide when to maintain, increase or restrict previous access where a user role changes. Access control must be supported by regular reviews to ensure that all authorised access to personal data is strictly necessary and justifiable for the performance of a function.

Particular attention should be paid to the deployment of IT administrator accounts with unrestricted access to personal data. Policies should be in place in regard to vetting and oversight of the staff members allocated these accounts. A staff member with such responsibilities should have separate user and administrator accounts. Multiple independent levels of authentication may be appropriate where administrators have advanced or extra access to personal data or where they have access or control of other’s account or security data.

There should be strict controls on the ability to download personal data from an organisation's systems. Such downloading can be blocked by technical means (disabling drives, isolating network areas or segments, etc.). Many organisations have taken a

decision to block access to USB ports having examined the inherent risks involved in leaving such ports open by default for all users.

Access Authentication

Users should have a unique identifier, such as a password, passphrase, smart card, or other token, to allow access to personal data. These are just examples, not an exhaustive list; for example, a biometric (e.g. a fingerprint, voice or retina scan) can also be used as a unique identifier. However, as biometrics in themselves raise serious data protection and privacy issues, their use should only be considered where other authentication methods are demonstrably insufficient.

Passwords / Passphrases

Passwords are a word or string of characters. A strong password should include a minimum of twelve characters (the longer the password, the harder it is for a computer to guess) and may contain one or more of the following:

- letters (upper and lower case);
- symbols (e.g. &, *, @, €, $, etc.);
- numbers (0 - 9); and
- punctuation (?, ", !).

However, users should not be required to use a mix of many types of character, as a strong password can be created using only one type of character (e.g. letters) once it is sufficiently long and hard to guess (for computers as well as people). Passwords should be reasonably easy for the user to remember but very difficult for anyone else to guess. Examples might include:

- M1_s?n, "The_^v1at#r"! (based on 'My son, "the aviator"!' with random characters replacing certain vowels or other letters)
- Te@m5Rb@dp@55word5 (based on 'Teams are bad passwords' with numbers and symbols replacing certain letters)

Please do not use these examples as actual passwords!

Passwords should not contain values known to be commonly-used or expected in passwords, or those which have been compromised. For example, users might be limited from using passwords which including, but not limited to:

- Passwords obtained from previous breaches;
- Dictionary words;
- Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’);

- Context-specific words, such as the name of the service, the username, or derivatives thereof.

Passphrases are similar to passwords, but represent a sentence or sequence of words. They should include twenty characters or more and may also include symbols, numbers and punctuation marks, e.g.

- "I Love the musical, The Sound of Music 2!"
- Ilike2swim@thelocalswimingpool

Data controllers should enforce password complexity and length, such as through rules that ensure that weak passwords and reused passwords are rejected. Users should not be required to change their password or passphrase arbitrarily (e.g. too frequently), as this can actually reduce password security (for example, by increasing reliance on simple passwords or reusing passwords). However, users should be required to change their password or passphrase if there is evidence it has been compromised or revealed, or when there is some other change in risk. Data controllers should never store users' passwords as plain text but should use strong and irreversible cryptographic hashing and salting to protect them and to allow secure checking for login purposes.

Data controllers should ensure that users are made aware that their password/passphrase is unique to them and must not be disclosed to anyone else. Shared credentials (where multiple users use the same login and password) should never be permitted. Vendor supplied defaults for system passwords and other security parameters should never be left in place. Data controllers must ensure that partner organisations with access to their systems or personal data respect these controls. Where possible, data controllers should promote password diversity by reminding users of the risks associated with password reuse across other internet services.

Multi-Factor Authentication

Multi-factor authentication (MFA) refers to there being more than one identity factor employed for access authentication. A commonly used option in many services is '2FA', which means that two factors for authentication are used. For example, instead of just using a password of their choosing, a user may have a second factor such as a biometric (e.g. a fingerprint scanner), or an "out-of-band" or alternative communication channel send a passcode to a secondary email address, phone number, or device. It should be noted, however, that some of these secondary channels are more secure than others

Devices such as smart cards or tokens, as well as standalone mobile apps, can be used as part of MFA, to provide authentication either by generating a code to be entered or containing a chip that authenticates with the system being accessed. They may generate a PIN number that is valid for a very short period of time. This is used in conjunction

with a username and password to authenticate the user, and can reduce the risk of 'brute force' password attacks or attacks where passwords have been stolen.

Automatic Screen Savers

Most systems allow for screensavers to activate after a period of inactivity on a computer, requiring a password to re-establish access. This automatic lock activation is useful as the alternative manual locking of a workstation requires positive action by the user every time he/she leaves the computer unattended.

Regardless of which method an organisation employs, computers should be locked when unattended. This applies not just to computers in public areas, but to all computers. It is pointless having an access control system in place if unattended computers may be accessed by any staff member, or where a shared password is used.

Encryption

Encryption is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network. As with passwords, this measure is pointless unless the key to decrypt the data is kept secure. The key should meet the standards of complexity required for passwords as discussed above.

In view of the rapid rate of technological development, it is not possible to be prescriptive about the standard of encryption that would ensure that data is inaccessible to unauthorised individuals. At present, 256 bit whole disk encryption would be viewed as an acceptable standard. We acknowledge that the market is bringing forward other options to securely encrypt data which may not require whole disk encryption and where properly applied by the user these can achieve the same security outcome.

Anti-Virus Software

Anti-virus software is not only required to prevent infection from the internet (either email or web-sourced) but to prevent viruses that may also be introduced from portable devices, such as memory sticks (the use of which should be strictly limited). No anti-virus package will prevent all infections, as they are only updated in response to infections. It is essential that such software is updated on a regular basis and that policies support vigilance in regard to potential threats. A policy of not opening email attachments from unexpected sources can be a useful way of preventing infection.

Firewalls

A firewall is essential where there is any external connectivity, either to other networks or to the internet. It is important that firewalls are properly configured, as they are a key weapon in combating unauthorised access attempts. The importance of firewalls has increased as organisations and individuals avail of "always-on" internet connections, exposing themselves to a greater possibility of attack.

Software Patching

Patches are the latest updates from the creator of your operating system software or application software. They usually contain fixes to potential security concerns and can be an important tool in preventing hacking or malware attacks. Organisations should ensure that they have regular, consistent and comprehensive patch management procedures in place.

Where possible, before installing the very latest patches, it is good practice to install these patches in a test environment to ensure that the patches do not create other issues with your systems. A record should also be kept of the date and patch installed on a system.

Remote Access

Where a staff member/contractor is allowed to access the network from a remote location (e.g. from home or from an off-site visit), such access creates a potential weakness in the system, not least when accessed from a wireless network. For this reason the need for such access should be properly assessed and security measures reassessed before remote access is granted. If feasible, the access should be limited to specific IP addresses. Security should be the first consideration in granting access to partner organisations.

Technical security measures, security assessments, contractual agreements in line with the requirements of the GDPR and the Data Protection Act 2018, and agreed standards of management of shared assets are all important aspects in managing this risk. It is the responsibility of the data controller to ensure that, regardless of the means by which a user remotely accesses their system, the security of the system cannot be compromised. Multifactor authentication for such access should be considered in this context.

Wireless Networks

Access to a server by means of a wireless connection can expose a network to attack. The physical environment in which such systems are operated may also be a factor in determining whether weaknesses in the system security exist. As with remote access, wireless networks should be assessed on security grounds rather than solely on apparent ease of use. Data controllers must ensure that adequate security is in place on the network through, for example, appropriate encryption measures or specification of authorised devices.

Particular vulnerabilities are associated with the use of third party unsecured WiFi networks (e.g. those provided in airports, hotels, etc.). A device using such a network may be open to attacks from other machines on the network. A good firewall should be installed on the portable device to prevent such attacks. The device should only connect to the network when necessary. When using unsecured WiFi to transmit personal or sensitive data, a secure web session should be in place to protect the data.

Portable Devices

Laptops, USB keys, smartphones, and other forms of portable device are especially vulnerable to theft and accidental loss. Where a data controller considers it essential to store personal data on a portable device, these devices should be encrypted. Whole disk encryption should be used to mitigate against storage of files outside of an encrypted segment of the disk.

In the case of smartphones, a strong password should be required at start up and also after several minutes of inactivity. When such a device is lost steps should be taken immediately to ensure that the remote memory wipe facility is activated. Staff allocated such devices should be familiar with the relevant procedures.

Logs and Audit Trails

Access control systems and security policies are undermined if the system cannot identify abuses. Consequently, a system should be able to identify the user name that accessed a file and the time of the access. A log of alterations made, along with author / editor, should also be created.

Logs and audit trails can help in the effective administration of the security system and can deter staff members tempted to abuse the system. Staff should be informed that logging is in place and that user logs are regularly reviewed. Monitoring processes should focus not only on networks, operating systems, intruder detection systems and

firewalls, but should include remote access services, web applications and databases. Logging systems can generate lots of information and an automatic means such as a System Information Event Monitor (SIEM) to filter and alert security staff about irregular audit trail entries may assist in its effective use.

An intruder detection system (IDS) acts as an internal alarm system that monitors and reports on malicious activities on a network or system. Such systems also aim to detect attacks that originate from within the system. Any organisation processing large volumes of personal data should have an IDS deployed and activated. Where alerts/events are generated by any such systems there must be a meaningful system in place to examine them in a timely fashion. This is to assist in identifying unusual activity and take immediate corrective action if there is an ongoing breach of security.

Back-Up Systems

A back-up system is an essential means of recovering from the loss or destruction of data. While some system should be in place, the frequency and nature of back up will depend, amongst other factors, on the type of organisation and the nature of data being processed. The security standards for back-up data are the same as for live data.

Incident Response Plans

Even with the best designed systems, mistakes can happen. As part of a data security policy, an organisation should anticipate what it would do if there were a data breach so that it can be ready to respond. Some questions you might ask yourself:

- ✓ What would your organisation do if it had a data breach incident?
- ✓ Have you a policy in place that specifies what a data breach is? (It is not just lost USB keys/disks/laptops. It may include any loss of control over personal data entrusted to organisations, including inappropriate access to personal data on your systems, or the sending of personal data to the wrong individuals).
- ✓ How would you know that your organisation had suffered a data breach? Does the organisation's staff (at all levels) understand the implications of losing personal data?
- ✓ Has your organisation specified whom staff tell if they have lost control of personal data?
- ✓ Does your policy make clear who is responsible for dealing with an incident?
- ✓ Does your policy cover the requirements of mandatory breach reporting (where applicable) under the Data Protection Act 2018, the GDPR, and/or the ePrivacy

Regulations (SI 336/2011) (including new availability and resilience requirements)?

Disposal of Equipment

When disposing of obsolete or redundant equipment many data controllers offer the equipment for sale to staff or donate it to charities. It is the responsibility of the data controller to ensure that all data previously stored on the devices has been removed prior to disposal. It is not sufficient to merely format the hard drives of the devices, as data can still be retrieved. Software is available that will overwrite the contents of the hard drive with a series of 1's and 0's to ensure that previous data cannot be retrieved. Dependant on the nature of the data stored, it is recommended that hard drives should be overwritten between three and five times.

Where the devices are not being recycled/reused the hard drives can either be physically destroyed or degaussed (a method of erasing data from a magnetic storage device).

It is important to consider the different types of equipment that may hold personal data. Besides obvious examples, such as servers, computers and laptops, there are a number of other devices that may store personal data. These may include smart phones, digital photocopiers, fax machines etc. Any data stored on these devices must also be erased prior to disposal.

Physical Security

In addition to technical security measures, data controllers must also consider the physical security measures which are necessary to ensure the security and integrity of any personal data they process. When assessing physical security needs, data controllers should consider a number safeguards, including, but not limited to:

- perimeter security (monitoring of access, office locked and alarmed when not in use);
- restrictions on access to sensitive areas within the building (such as server rooms);
- computer location (so that the screen may not be viewed by members of the public);
- storage of files (files not stored in public areas with access restricted to staff with a need to access particular files); and
- secure disposal of records (effective "wiping" of data stored electronically; secure disposal of paper records).

The Human Factor

No matter what technical or physical controls are placed on a system, the most important security measure is to ensure that staff are aware of their responsibilities. Passwords should not be written down and left in convenient places; passwords should not be shared amongst colleagues; and unexpected email attachments should not be opened unless first screened by anti-virus software. Effective employee training about the risks of data compromise, their role in preventing it and how to respond in the event of problems can be a very effective line of defence. Many organisations set security policies and procedures but fail to implement them consistently. Running scenario based training sessions may assist in effective training.

Controls focused on individual and organisational accountability and ensuring that policies are carried out are an important part of any system designed to protect personal data. Identify essential controls first and ensure that these controls are implemented across the organisation without exception. Once this is in place, move on to more advanced controls designed to mitigate the risks specific to the organisation and the type(s) of data processed.

Data controllers must have procedures in place to manage staff turnover, including retrieval of data storage devices and quick removal of access permissions.

Certification

Certification can be a useful means of demonstrating compliance with security obligations, where certification indicates that data security controls have been subject to audit or review against a recognised standard by a reputable third party organisation. In the context of cloud computing, customers should look to see whether cloud services providers can provide a copy of this third party audit certificate and review the date and the scope of the certification.

Where cloud service providers offer model clauses, a relevant third party audit report may satisfy in lieu of an individual right to audit. Individual audits of data hosted in a multi-party, virtualised server environments may be impractical technically and in fact serve to increase risks to those physical and logical network security controls in place. However, it remains up to the data controller to ensure they are satisfied with security provisions made, and to determine how they can demonstrate this if required.