ICAEW KNOW-HOW
BUSINESS LAW
GDPR AND THE DATA PROTECTION ACT 2018

PERSONAL DATA BREACHES

GUIDE

January 2020

The Data Protection Act 2018 (DPA 2018) came into force on 25 May 2018 to replace the Data Protection Act 1998. It sits alongside the General Data Protection Regulation (GDPR). This guide is part of a series that explain some of the new or more difficult concepts introduced by the DPA 2018 and the GDPR. It is intended to provide practical guidance to ICAEW members. It is not intended to constitute legal advice. If in doubt members should contact the Information Commissioner's Office (ICO) and/or seek independent legal advice.

Introduction

The GDPR makes it mandatory for data controllers to report certain types of personal data breaches to the relevant supervisory authority (the Information Commissioner's Office (ICO) in the UK) and (in some instances) to the data subjects affected. The GDPR also sets out a specific timeframe for notification, ie, without undue delay and, where feasible, no later than 72 hours of when you become aware of the breach.

This guide gives you a framework to understand what a personal data breach is and your obligations should a data breach occur. It does not tell you what to do as your response will vary according to the circumstances of each breach, though it does provide some guidance on what may be appropriate in certain circumstances. Even if you consider a breach to be similar to the examples given, you should still consider each breach and your response to it on a case by case basis. You are accountable for your own decisions and must be able to explain what you have done and why.

If you are unsure of the correct action to take, you can contact the ICO's confidential helpline (0303 123 113), who will discuss the breach with you in more detail.

Please remember that this guidance applies only to personal data breaches and your responsibilities under the DPA 2018 and the GDPR in the event of such a breach. A breach may also involve other confidential and/or commercially sensitive information in which case you should consider the appropriate action to take to recover the information and / or mitigate the loss.

What is a personal data breach?

Article 4(12) of the GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

It may also be useful to consider a personal data breach as falling into one or more of the following categories:

- **Confidentiality breach** – where there is an unauthorised or accidental disclosure of, or access to, personal data.

Example: An email with the personal data of a client's employees, including name, address, salary, national insurance number and date of birth, was inadvertently sent to the wrong client.

- **Integrity breach** – where there is an unauthorised or accidental alteration of personal data.

  Example: A client calls to amend their contact details. The wrong client's contact details are updated by accident. (This could also lead to a confidentiality breach when the wrong client was then contacted with details relating to the other client.)

- **Availability breach** – where there is an unauthorised or accidental loss of access to, or destruction of, personal data.

  Example: A cyber incident means that the client database is accidentally deleted. The login details to access the HMRC portal are lost.

Other infringements of GDPR may amount to a breach of the law, but if they do not meet the Article 4 (12) definition they will not constitute a personal data breach (and therefore will not be subject to the reporting requirements, which are specific to personal data breaches).

Examples of other breaches include:

- Failure to respond to a subject access request on time.
- Sending marketing information to individuals without their consent (but this may be a breach of Privacy and Electronic Communications Regulations (PECR)).
- Loss of data about a deceased individual (as GDPR only applies to living people), unless the data loss could also have an impact on a living person.

When do you become 'aware' of a personal data breach?

The 72-hour timeframe for reporting a breach to the ICO will begin as soon as the data controller is "aware" that personal data has been compromised. The European Data Protection Board ("EDPB", previously Article 29 Working Party) guidance states that a data controller is "aware" when they have "a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised." It may be that the data controller is not aware until sometime after the breach occurred. However, they would be expected to be in control of the personal data they are processing and so a long delay would likely have to be explained in any notification to the ICO.

In situations where the personal data breach takes place with a data processor, the data controller becomes "aware" of the personal data breach when the data processor notifies them.

What are my obligations if there is a personal data breach?

Your obligations will vary dependent on whether you are a data controller or data processor. You may be either a data controller or a data processor depending on the data processing in any scenario. Further information on data controllers and data processors can be found in the ICAEW Know-How *Data Controllers v Data Processors*

As above, a data controller is required to notify the regulator without undue delay and, where feasible within 72 hours after having become aware of it. The controller must communicate the personal data breach to data subjects, again without undue delay, where it is likely to result in a high risk to their rights and freedoms.

The 72-hour timeframe imposed by the GDPR and the need to act without undue delay does not take into consideration weekends and bank holidays. Therefore, if a data controller becomes

aware of a breach at 5.00pm on a Friday, they still need to be able to take appropriate action within 72 hours.

A data processor is required to notify the data controller without undue delay after having become aware of a data breach.

What are the obligations on data controllers in the event of a personal data breach?

Data controllers are subject to four obligations – Record, Notify, Communicate, Contain and Mitigate:

Record (Article 33 (5))

All personal data breaches are required to be recorded internally irrespective of whether they are required to be notified to the ICO or communicated to the data subjects.

Notify (Article 33)

Personal data breaches are required to be notified to the ICO (or any other relevant supervisory authority) "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." The notification should be made by the organisation's Data Protection Officer (DPO) if appointed. If the organisation does not have a DPO, then the notification should be made by the member of the management team responsible for data protection issues.

The ICO has provided a Personal data breach reporting template and a confidential helpline (0303 123 1113) should you be unsure whether to notify the breach or about any of the questions within the template.

Notifications should include:

1. The nature of the breach including the categories and numbers of data subjects affected;
2. The name and contact details of the Data Protection Officer (DPO) or relevant contact;
3. The consequences of the breach; and
4. Details of measures taken to address the breach and, where appropriate, to mitigate its possible adverse effects.

Notifications to the ICO are required without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If not all the information is available within 72 hours of becoming aware of the breach, a notification should still be made to the ICO with the details currently available, and then a full notification can be made as soon as the information does become available.

If a decision is made that a notification to the ICO is not required, the reasoning behind this decision must be documented. The ICO can impose sanctions on data controllers who fail to notify them of data breaches when it is necessary to do so.

Regardless of any necessary ICO notification, an organisation should also consider whether there are any other regulatory bodies which would require notification. These could include for example the Financial Conduct Authority, Prudential Regulation Authority or other financial crime bodies. Other third parties such as the police, HMRC, insurers, banks or credit card companies may also require notification of the breach. Post Brexit an organisation may also need to inform their EU representative.

A data controller may also have contractual notification obligations. Controllers should consider whether they might be obliged to notify the client or a third party as a result of any contractual

obligations and whether their contractual obligations might be more onerous than their legal obligations.

Communicate (Article 34)

Where the breach is "likely to result in a high risk to the rights and freedoms of natural persons", the data controller should inform the data subjects (individuals) concerned without undue delay. The main reason for informing individuals is to help them take steps to protect themselves from the effects of a breach, such as changing passwords or monitoring credit card or bank accounts for unusual transactions. The data controller should inform the affected data subjects of the following:

1. the nature of the breach, including the categories and numbers of data subjects affected;
2. the name and contact details of the Data Protection Officer (DPO) or other contact point;
3. the likely consequences of the breach;
4. details of recommended measures that should be taken by individuals to mitigate possible adverse impacts of the breach; and
5. if appropriate, it may also be helpful to reassure the individual to explain that you have rectified the cause of the breach and steps put in place to prevent it occurring again.

The data controller should make sure that any decision not to communicate to the individual is documented. You may still need to notify the ICO of the breach unless you can demonstrate that it is unlikely to result in a risk to the rights and freedoms of natural persons. Members should also be aware that the ICO can compel an organisation to disclose to data subjects that a breach has occurred.

Even if the decision is taken that there is no legal obligation to communicate to individuals, you may wish to consider whether you might want to inform individuals of the breach in any event in order to maintain or protect your client relationship.

Contain and mitigate (Article 33(3)(d))

Data controllers have an obligation to ensure that any personal data breach is contained as quickly as possible and that any potential risks to the individuals concerned are appropriately mitigated. This will include taking action to correct the vulnerabilities that gave rise to the breach as well as putting appropriate technical and organisation measures in place to prevent recurrence.

All data controllers should consider their ability to deal with any personal breaches and formulate a response plan.

Appropriate escalation procedures should be in place to ensure that in the event of a serious personal data breach the appropriate persons (such as the board of directors, senior management team) are notified of both the breach and the implications of failing to act (including failure to notify the ICO and /or data subjects).

See Appendix 1 for a summary of the obligations of Data Controllers and Data Processors in the event of a personal data breach.

What does a data processor have to do in the event of a personal data breach?

A data processor has an obligation to notify the data controller without undue delay after becoming aware of a personal data breach (Article 33 (2)).

Data processors will also be required to assist in any investigation so that the data controller has appropriate knowledge of the facts surrounding the personal data breach in order that they can meet their obligations in recording, notifying or communicating as required.

A data processor may also have assumed contractual notification obligations more onerous than their legal obligations. For example, they may have to notify the data controller within 24 hours.

See Appendix 1 for a summary of the obligations of data controllers and data processors in the event of a personal data breach.

What are the factors to consider when assessing the risk related to a personal data breach?

Each breach **MUST** be assessed on a case by case basis as every situation will be different. Guidance has been issued by the ICO here and by the EDPB (previously Article 29 Working Party) here.

When assessing risk, an organisation should consider the likelihood and severity of the risk to the rights and freedoms of data subjects, not the risk to the organisation. Things to consider include data volume, data sensitivity, intent and severity of consequences for those individuals affected. A combination of personal data is typically more sensitive than a single piece of personal data and more likely to result in a higher risk. Breaches of *special categories of personal data* are generally considered to be likely to result in a high risk to the rights and freedoms of the individual.

Factors to consider

The following is a non-exhaustive list of factors to consider when determining the level of risk in a number of scenarios that members may encounter.

1. **An email is sent to an incorrect recipient.**

   Consider: What personal data is contained in the email? How much personal data was involved? Were there any attachments? If so, were they password protected or encrypted? If the data contained within the email were to get into the wrong hands, could it be used to commit identity fraud? What is the likelihood of this, ie, who is the recipient – could they be considered a trusted third party (see below)? Has confirmation of deletion been received?

   Examples:

   - *An email with little personal data, accidentally sent to a trusted third party (see below) is unlikely to require notification to the ICO or the individual.*
   - *An email with considerable personal data or to an unknown recipient is more likely to require notification to the ICO and, possibly, communicated to the data subjects concerned.*
   - *An email containing personal data only within encrypted attachments for which the password/decryption key is unknown to the recipient is unlikely to need notification.*
   - *If the email contains personal data relating to a client, you may want to consider whether to notify them from a client service perspective in any event.*

2. **Management information regarding employees is sent to the wrong parties.**

   Consider: How quickly was the error was spotted and how quickly was the breach contained? What type of personal data was involved and how much? How many parties was it incorrectly sent to and who were they? Has the incident been successfully contained, and incorrect emails deleted?

   Examples:

- *If the information was sent internally to single individual in another department in the organisation and promptly deleted, then the risk to the individuals may be considered low and no notification required.*
- *If the information contained extensive personal data and was inadvertently sent to a large number of recipients, then it is likely to require notification to the ICO as well as communication to the data subjects involved – especially if special categories of personal data are involved.*

3. An employee clicks on a link in a phishing email and enters their log on details. As a result of this, there is evidence of unauthorised access to the mailbox.

Consider: What personal data is contained within the mailbox and what is the risk to each individual concerned? How much personal data is in the mailbox for each individual? What type of personal data? Is there evidence to show data has been extracted from the mailbox? How long will it take to complete the risk assessment?

Examples:

- *Anti-Money Laundering "Know Your Customer" personal data, for example, will be much more likely to result in a higher risk to an individual than their date of birth alone. However, their date of birth together with just one other element of personal data could also increase the likelihood of risk and require notification to the ICO.*
- *If it will take considerable time to determine all the personal data in the mailbox and complete an assessment of the risk, you should consider making a preliminary notification to alert the ICO and, possibly, even the individuals to the situation. Once more information is known, an updated report can be made.*

4. An employee working out their notice period emails clients' personal data to their own personal email account.

Consider: What was the type and volume of the clients' personal data? Is the employee leaving on good terms? Will they delete the emails, allow their mailbox to be searched, and confirm in writing that they have deleted the data and not distributed it further? How long ago did they send the personal data? Could they already have been forwarded on and out of your control? Do you have evidence of what was sent? What is the reason the employee forwarded the emails?

Examples:

- *If the personal data is not sensitive and the employee acknowledges the error and confirms that the personal data has been deleted and not distributed further, it may be possible to determine that the incident has been contained and that there is unlikely to be a risk to the clients. In such circumstances, the ICO need not be notified.*
- *If the employee was selective in the details forwarded, they may be intending to poach clients, and so there may be deemed to be a risk to the clients (ignoring the fact that it would likely be a breach of the employees restrictive covenants).*
- *If the employee forwarded information indiscriminately with no clear reasoning, then this may constitute a personal data breach and require notification to the ICO and/or to individuals.*

In addition to the data breach reporting requirements, members should be aware that the ICO may wish to investigate situations where employees have sent personal data (especially special category personal data or data relating to vulnerable groups) to their own email accounts without authorisation and, where deemed appropriate, prosecute the individuals

concerned for breaching data protection legislation. Details of ICO actions taken against individuals in such circumstances is available on the ICO website *Action we have taken*.

5. A third-party software as a service provider advises you that they have experienced a personal data breach concerning your clients' data.

Consider: Has the data processor managed to contain the breach? What was the nature of the breach? Was the breach as a result of a malicious attack? What data was contained in the breach and how much? What could be the potential impact on the data subjects concerned? Has the data processor made any notifications?

Examples:

- *Access controls for a collaboration platform were found to contain a vulnerability that could allow access by one client to another client's data. If the vulnerability was corrected immediately and a review of access logs indicated that no unauthorised access attempts were made, then there is unlikely to be any impact on any individuals and no notification required.*
- *A personal tax return preparation service provider informs you that all your clients' tax details have potentially been compromised and exposed to unknown third parties, albeit investigations are continuing. This is likely to require initial notification to the ICO, which can be updated as the results of the additional investigations become known. Communication of the breach to your affected clients may also be required.*

Be aware that when considering the appropriate action to take in respect of a personal data breach, the conditions of any relevant insurance policy may also be relevant.

See Appendix 2 below for a Decision Tree to help you assess whether you need to notify the ICO and data subjects. The ICO's webpage *Action we have taken* is a good indication of the type of activity that is considered a breach by the ICO. The EDPB's *Guidelines on Personal data breach notification* also contains helpful material in determining when a breach might result in a risk to individuals.

What if the personal data breach involves 'trusted' third parties?

In assessing the severity of consequences for individuals, the EDPB "Guidelines on Personal data breach notification" allow the concept of 'trusted' third parties. Where a data breach occurs and personal data is disclosed to a third party in error, that recipient may be another client, supplier or colleague. In such circumstances, the data controller will have an ongoing relationship with the recipient and may be aware of their procedures, history and other relevant details such that the recipient can be considered "trusted". In other words, the data controller may have a level of assurance with the recipient so that they can reasonably expect that party not to access, read or further disseminate the data sent in error, and to comply with instructions to return or delete it. This is very different to situations where the intention of the third party who has inadvertently received the personal data is unknown and/or possibly malicious. The extent of trust in the third party recipient can therefore be factored into the risk assessment the controller carries out following the breach; specifically, a trusted relationship may reduce the likelihood of risk to individuals and negate the need to notify the ICO or communicate to the individuals. It should however be noted that it does not mean that a breach has not occurred, and the breach and reasons for not notifying the ICO or communicating with individuals should still be documented.

Example:

- *A personal tax return is emailed by a member to the wrong client in error. The client notices that the data is for another client and confirms to the member that the email has been deleted and not disseminated further. There is a good, long standing relationship between*

the incorrect recipient and the member, and it is therefore reasonable to assume that the incorrect recipient can be trusted to have contained the breach. Notification to the ICO is therefore unlikely to be required.

What is the role of the data protection officer in a personal data breach?

When notifying the data breach to the ICO or communicating to data subjects, the data controller is required to provide the name and contact details of the Data Protection Officer (DPO) or other contact point. This is irrespective of whether a DPO is required by Article 37 or has been appointed on a voluntary basis as a matter of good practice.

The DPO acts as the contact point and conduit between the data controller and the ICO and the data subjects. As such the DPO needs to be promptly informed about the existence of a breach and involved throughout the breach management and notification process. The DPO should also play a key role in assisting the prevention of breaches and preparation of breach contingency plans by providing advice and monitoring compliance, as well as during a breach (ie, when notifying the ICO or other supervisory authority), and during any subsequent investigation.

What is the best way to avoid and mitigate a personal data breach?

It is probably impossible to eliminate the risk of ever facing a personal data breach, but you can take action to minimise the risk of one occurring and, should a breach occur, to mitigate its impact. These include:

- Ensuring your staff are well-informed of what constitutes a personal data breach, the data handling controls and procedures they should adopt to prevent a breach and are aware of how to report a data breach within your organisation through a defined process.
- Providing regular data protection training to all staff.
- Regularly reviewing, testing and updating as necessary your information and cyber security policies and procedures.
- Implementing privacy by default and design and conducting Privacy Impact Assessments.
- Regularly reviewing, testing and updating as necessary your breach response plan.
- Acting swiftly to take mitigating actions. These will vary according to the situation, but may include obtaining confirmation of deletion of communications sent to incorrect recipients or from individuals known to have emailed data to their personal email accounts without authorisation, removing access rights from a breached systems, informing impacted individuals of the breach and recommending they take appropriate actions (eg, changing passwords), and review of activity logs to understand the scope of a breach.

Where can I find out more?

The ICO has provided a Personal data breach reporting template.

The ICO also has a confidential helpline (0303 123 1113) should you be unsure whether to notify the breach or about any of the questions within the reporting template.

For detailed advice read:

- EU General Data Protection Regulations (GDPR)
- Data Protection Act 2018 (DPA 2018)
- The ICO's guidance on Personal Data Breaches
- The European Data Protection Board's (formerly the Article 29 Data Protection Working Party) guidance on when to notify data breaches

For more general advice on all aspects of the DPA 2018 and GDPR, see the ICO's Guide to Data Protection.

For more member support, visit ICAEW's GDPR hub and Data Protection webpages and access the Technical Advisory Service Practice Helpsheets on GDPR and Data Protection.

For advice on what to do in the case of a cyber-attack see ICAEW's Cyber Security hub.

APPENDIX 1 – Summary of data controller and data processor obligations in the event of a personal data breach

Controller Obligations
Data containment and mitigation of breach
Record details of the breach
Notify ICO without undue delay & within 72 hours (and record the decision-making process even if notification is not considered appropriate)
Communicate to the individual without undue delay (if appropriate)
Processor Obligations
Data containment and mitigation of breach
Notify the Controller without undue delay
Assist with any subsequent investigation
Consider any other regulatory or contractual obligations

APPENDIX 2 – Data Breaches Decision Tree

NB This Decision Tree only gives suggested actions in the particular situation outlined. It does not provide details of all the actions required for every type of breach. The action required when a breach occurs will vary according to the specific circumstances of that breach and so must be decided on a case by case basis.

Nature of breach	Context	Type of personal data					Type of breach			Notify ICO	Communicate to data subjects
		Limited personal data	Bank account/Credit card	Government ID	Special Category data	Criminal conviction data	Confidentiality	Integrity	Availability		
Email sent to incorrect recipient	Sent to "trusted" third party Deletion/non-disclosure confirmation received Unencrypted	✓	✗	✗	✗	✗	✓	✗	✗	No	No
		✗	✓	✓	✓	✓	✓	✗	✗	Consider	Consider
	Sent to unknown recipient No deletion/non-disclosure confirmation received Unencrypted	✓	✗	✗	✗	✗	✓	✗	✗	Consider	No
		✗	✓	✓	✓	✓	✓	✗	✗	Yes	Yes
	Sent to unknown recipient No deletion/non-disclosure confirmation received Encrypted	✓	✓	✓	✓	✓	✓	✗	✗	No	No
Loss of hard copy documents		✓	✗	✗	✗	✗	✓	✗	✓	No	No
		✗	✓	✓	✓	✓	✓	✗	✓	Yes	Consider
Email containing personal data sent by employee to their personal webmail address	Current employee (not leaving) Transfer of data explainable (eg to work on data at home) Deletion/non-disclosure confirmation received	✓	✓	✓	✓	✓	✓	✗	✗	No	No
	Current employee (imminent leaver) No rational explanation for data transfer Deletion/non-disclosure confirmation received	✓	✗	✗	✗	✗	✓	✗	✗	No	No
		✗	✓	✓	✓	✓	✓	✗	✗	Yes	Yes
	Current employee (imminent leaver) No rational explanation for data transfer No deletion/non-disclosure confirmation received	✓	✗	✗	✗	✗	✓	✗	✗	No	No
		✗	✓	✓	✓	✓	✓	✗	✗	Yes	Yes
Large volume of personal data sent to client by email unencrypted	Encrypted in transit (Transport Layer Security in place)	✓	✓	✓	✓	✓	✓	✗	✗	No	No
	No encryption in transit (Transport Layer Security not in place)	✓	✗	✗	✗	✗	✓	✗	✗	No	No
		✗	✓	✓	✓	✓	✓	✗	✗	Yes	Consider

There are over 1.8m chartered accountants and students around the world − talented, ethical and committed professionals who use their expertise to ensure we have a successful and sustainable future.

Over 180,000 of these are ICAEW Chartered Accountants and students. We train, develop and support each one of them so that they have the knowledge and values to help build local and global economies that are sustainable, accountable and fair.

We've been at the heart of the accountancy profession since we were founded in 1880 to ensure trust in business. We share our knowledge and insight with governments, regulators and business leaders worldwide as we believe accountancy is a force for positive economic change across the world.

ICAEW is a founder member of Chartered Accountants Worldwide and the Global Accounting Alliance.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

T +44 (0)20 7920 8100
E generalenquiries@icaew.com