

**GDPR TEMPLATE:**

**GUIDE TO HANDLING A PERSONAL DATA BREACH**

**Points to note**

* Before using this template Guide to Handling a Personal Data Breach, it is essential that you read these ‘Points to note’, together with the separate document, ‘Make UK Essential GDPR Templates for HR – Points to note’, which provides important information applicable to all of the template documents, including this Guide.
* This Guide is effectively a template internal process for handling personal data breaches. It is intended to provide senior managers/HR with a detailed explanation of how to handle a personal data breach in accordance with the UK GDPR requirement to notify the Information Commissioner’s Office (ICO) and, potentially, affected individuals and to record details of the breach. It is not intended to be distributed to all staff.
* Taking into account the security implications of a personal data breach, our recommendation would be that the compliance procedures and related decision-making set out in this Guide should be confined to senior managers/HR (in collaboration with Data Protection Officer/Data Protection Team/Data Protection Lead).
* Although this Guide is not designed to be distributed throughout the workforce, it is very important that all staff are trained to be able to identify a potential personal data breach. They must also be made aware of what the employer expects of them when they identify a breach and how to alert the appropriate bodies. These expectations and obligations apply to any personal data breach, whether it concerns other employees, customers, suppliers, or other third parties. We therefore recommend that employers also have in place an organisation-wide data protection policy, such as our GDPR Template: Data Protection Policy, which (among other things) sets out these requirements and emphasises their importance. We would also suggest that employers reinforce these messages through regular staff training.
* There is no express statutory obligation to have a written process, such as this Guide, for handling personal data breaches. However, it is recommended as good practice in guidance produced by the ICO, including the Accountability Framework (available here: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/breach-response-and-monitoring/>).
* The definition of ‘special category data’ which has been used in this Guide includes data relating to individuals’ criminal convictions or offences data. While the UK GDPR definition of ‘special category data’ does not include this type of data, under the DPA 2018 many of the same safeguards apply and, therefore, for practical purposes we have included this type of data in the Guide’s definition of ‘special category data’.
* This Guide assists in satisfying broader obligations under the GDPR to *demonstrate* compliance with data protection law (referred to as the ‘accountability’ principle). It can also be described as an *organisational measure* that helps the employer to ensure data protection compliance *by design and by default* by seeking to avoid compliance failure through lack of knowledge and poor procedure when handling a personal data breach.
* The content of this Guide draws significantly on ICO guidance (in force as at October 2023). Much of the Guide is self-explanatory. However, where there are particular tricky issues, or the ICO guidance lacks clarity, we have highlighted this and explained our recommended approach in the points set out below.
* **Additional compliance requirements:** This Guide focuses on requirements involving personal data breaches under the GDPR. However, depending on the nature of their business, organisations may also wish to customise the Guide to add reference to other particular provisions, e.g. if you are a communications service provider, you must notify the ICO of any personal data breach within 24 hours under the Privacy and Electronic Communications Regulations (PECR).
* **Cross-border breaches:** Occasionally, a personal data breach may involve the processing of personal data in more than one country (or may affect individuals based in more than one country).

The UK is no longer part of the EU GDPR’s ‘one-stop shop’ system that provided for the identification of and notification to a ‘lead supervisory authority’ (as opposed to requiring notification to all of the local supervisory authorities in the event of a personal data breach involving more than one EEA country). Reportable breaches that occur in/affect individuals in the UK will have to be reported to the ICO.

Companies that process personal data of individuals in EEA countries and that previously had the ICO as their lead supervisory authority should now have identified an alternative ‘lead supervisory authority’ to whom they will report personal data breaches affecting data subjects in EEA countries, if applicable. However, depending on their organisational structure and EEA data processing activities, the ‘one-stop shop’ system may not be applicable to certain companies. In the event of a personal data breach affecting data subjects in EEA countries, these companies may need to notify the local supervisory authority in each affected country. For further information on whether the concept of a lead supervisory authority is applicable to your organisational structure, please refer to the ICO guidance on EU regulatory oversight following the end of the transition period, which can be accessed here: <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/eu-regulatory-oversight/>. For information on determining which EU supervisory authority should be your lead supervisory authority, the European Data Protection Board (EDPB) have produced guidance which can be accessed from:

<http://ec.europa.eu/newsroom/document.cfm?doc_id=44102>.

**Guide to Handling a Personal Data Breach**

[COMPANY] takes all data protection breaches very seriously as the consequences for [COMPANY] and its workforce can be severe in terms of legal, financial and reputational damage.

Data protection law requires [COMPANY] to report certain data protection breaches known as ‘personal data breaches’ (see below for definition) to the UK data protection supervisory authority, the Information Commissioner’s Office (ICO), without undue delay and, where feasible, not later than 72 hours after becoming aware of it. In serious cases, [COMPANY] may also have to communicate details of the breach to the affected individuals. (In some cases which involve a cross-border breach, [COMPANY] may be required to report to the supervisory authority in the other affected country/countries).

Record keeping requirements also apply to all cases of personal data breaches.

[COMPANY’S] Data Protection Policy [, *which is available from/LINK,*] sets out what [COMPANY] expects of its Employees (including current and former employees, workers, contractors, agency workers, consultants, interns, volunteers, partners and directors) in relation to alerting [COMPANY] to breaches or suspected breaches of [COMPANY’S] Data Protection Policy, including personal data breaches.

This **Guide to Handling a Personal Data Breach** (the Guide) explains the necessary procedures that [*the Data Protection Team/Data Protection Officer/Managers*] must follow as soon as they have been alerted to a personal data breach or suspected personal data breach by an Employee or any other individual.

**What is a personal data breach?**

**Personal data**

Personal data means any information relating to a living individual (also known as a ‘data subject’) who can be identified (directly or indirectly), in particular by reference to an identifier (e.g. name, NI number, employee number, email address, physical features). Relevant individuals can include your colleagues, consumers, members of the public, business contacts, etc. Personal data can be factual (e.g. contact details or date of birth), an opinion about a person's actions or behaviour, or information that may otherwise impact on that individual. It can be personal or business-related.

Personal data may be automated (e.g. electronic records such as computer files or in emails) or contained in manual records which are part of a filing system (e.g. structured paper files and archives). Information that is stored in another way (such as in an unstructured file or in handwritten notes) can also be personal data if it is created with the intention that it will be stored electronically or in a filing system.

Some categories of personal data are ‘special’ because they are particularly sensitive. Special category data is personal data about an individual’s:

* racial or ethnic origin;
* political opinions;
* religious or philosophical beliefs;
* trade union membership;
* physical or mental health;
* sex life or sexual orientation;
* biometrics (if used for identification purposes) or genetics; and/or
* criminal offences or convictions.

**Personal data breach**

A personal data breach occurs where there has been 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.

This covers personal data that is controlled and/or processed by [COMPANY] (e.g. personal data stored on [COMPANY] electronic devices or manual files) or personal data processed by a third party (e.g. a payroll agent) on behalf of [COMPANY].

If a personal data breach was caused by a third party processing on [COMPANY]’s behalf, the third party processor must notify the breach to [COMPANY] without undue delay. However, [COMPANY] is still solely responsible for any notification of the breach to the ICO (and/or other relevant supervisory authority) and/or to affected individuals.

**Examples of personal data breaches**

Common examples of a personal data breach could include:

* A misdirected work email containing an Employee’s personal contact details;
* Theft of a mobile phone containing customer or Employee-related personal data;
* Accidental loss of an HR personnel file from an office at work or at home;
* A computer hack which involves the corruption of personal data across all [COMPANY] files;
* Temporary loss of a work iPad containing Employee or customer-related personal data in a public place;
* Unintentional disclosure of a payroll spreadsheet by leaving a copy on a photocopier where it can be viewed by unauthorised recipients;
* Accidental deletion of an Employee’s medical reports relating to a health and safety incident;
* Unauthorised and malicious amendments made to witness statements in a disciplinary file to assist an Employee’s case;
* Temporary unavailability of HR drives due to a serious power cut or denial of service attack (although note that a lack of availability due to planned system maintenance is not a personal data breach).

**What action should [COMPANY] take in relation to managing a personal data breach?**

As soon as a personal data breach or suspected personal data breach has been alerted to [HR/Senior Managers/the Data Protection Officer/the Data Protection Team/the Data Protection Lead], formulate an action plan to:

1. **Assign a lead individual** to take responsibility for overseeing the personal data breach management and notification;
2. **Investigate** whether there has been a personal data breach/the circumstances of the personal data breach and **assess** the level of associated risks to determine if the breach requires notification to the ICO (and/or other relevant supervisory authority) and, potentially, affected individuals;
3. **Consult specialists** across the business (e.g. IT, HR and Legal) and/or appropriate external consultants or law enforcement bodies (e.g. the police) for guidance on appropriate action to help contain any adverse effects of the breach and/or recover compromised personal data;
4. Take any necessary action for **containment and recovery** and carry out **notification** procedures, as required;
5. Complete **record-keeping** requirements and any **follow-up procedures**.

**Does [COMPANY] need to notify the personal data breach to the ICO (and/or other relevant supervisory authority)?**

Not all personal data breaches need to be notified to the ICO (or other relevant supervisory authority) (although they must be recorded [in the Internal Personal Data Breach Register] – see below).

Data protection law requires [COMPANY] to assess as soon as possible whether a breach should be notified. Only breaches which are likely to result in a risk to the rights and freedoms of individuals must be notified. As soon as you become aware of a personal data breach, [COMPANY] requires you to carry out a risk assessment by considering:

* *The type of breach*

(i.e. The level of risk where, for example, a portable electronic device has been stolen will be much higher than if it has been mislaid for a day at home and subsequently found.)

* *The nature, sensitivity, and volume of personal data*

(i.e. Names and addresses on a small contact list would, for example, ordinarily appear to be low risk, but if this is in fact a list of confidential complainants in relation to a sexual harassment investigation, it is potentially very damaging. Where a breach involves special category data, this can increase the likelihood of harm, and where a breach involves a large amount of personal data about many data subjects, this is also likely to increase the risk to individuals.)

* *Ease of identification of individuals*

(i.e. Check if identification of the personal data could be made easily (higher risk), or if it has been encrypted or password protected (lower risk).)

* *Severity of consequences for individuals*

(i.e. Could the breach result in identity theft, fraud, financial loss, physical harm, discrimination, loss of confidentiality, psychological distress, humiliation, or damage to reputation? Is there any special category data involved? Would the consequences have a long-term effect on individuals? For example, where information is accidentally disclosed to a trusted source who can be relied upon to delete the data or not to take any action, there may be no risk to individuals which requires notification.)

* *Special characteristics of the individual(s) affected or the source of the information?*

(i.e. Does the breach involve any vulnerable individuals and/or does it involve a sensitive source of information such as occupational health?)

* *The number of affected individuals*

(i.e. Although a breach can have a severe impact on just one individual, generally the larger the number of individuals affected, the more severe the personal data breach.)

When deciding whether to notify the ICO (and/or other relevant supervisory authority), take all of the above factors into account. Bear in mind the severity of the potential consequences of the personal data breach and also the actual likelihood of those consequences occurring. If you are unsure whether a particular breach needs to be reported, the ICO helpline can offer advice, although they will expect you to make your own decision on whether to report, on the basis of their advice and a proper consideration of the above factors. (The ICO helpline telephone number is +44 303 123 1113 and normal opening hours are Monday to Friday between 9am and 5pm.)

Regardless of your conclusion, ensure that you record your reasoning and decision in accordance with the requirements set out in the **Record-keeping** section below.

If you decide to notify the ICO (and/or other relevant supervisory authority), but further investigation reveals that any risk was contained or mitigated, such that there was no notifiable personal data breach, you should update the ICO (and/or other relevant supervisory authority). There is no penalty for making a notification that ultimately turns out not to have been required.

**To which supervisory authority should [COMPANY] notify the personal data breach?**

Where a personal data breach by [COMPANY] that is likely to result in a risk to the rights and freedoms of individuals occurs in relation to processing in the UK, it will be necessary to report the breach to the ICO. If the personal data breach is confined to the UK and does not have any cross-border elements, there will be no need to report it to any other supervisory authorities.

In some cases, however, a personal data breach by [COMPANY] may involve the processing of personal data in/affect individuals based in an EEA country or more than one EEA country.

[***IF YOU DO NOT HAVE A LEAD SUPERVISORY AUTHORITY BECAUSE IT IS NOT APPROPRIATE FOR YOUR ORGANISATIONAL STRUCTURE:*** In these circumstances, notification will need to be made to the supervisory authority in the EEA country or countries affected by the breach.]

[***OR, IF YOU HAVE A LEAD SUPERVISORY AUTHORITY:*** In these circumstances, notification will need to be made to the [COMPANY] Group’s ‘lead supervisory authority’ (i.e. the supervisory authority of the EEA country in which [our central administration in the EEA is located]), which is [i*nsert details*]. You should therefore notify [*insert lead supervisory authority*] via [*lead supervisory authority contact details*]in the event of a notifiable personal data breach involving one or more EEA countries.]

If a personal data breach by [COMPANY] occurs in a non-EEA country or affects individuals in a non-EEA country, it may be necessary to report the breach to the local data protection authority in the relevant country. The rules regarding notification of personal data breaches in non-EEA countries are outside the scope of this Guide. However, [COMPANY] should not delay in obtaining advice, where there is uncertainty, to avoid any potential penalties.

**What action should [COMPANY] take to help contain the adverse effects of a personal data breach or recover compromised personal data?**

The focus of the legal requirement to notify personal data breaches is to limit damage to individuals by acting promptly to contain a breach and, if possible, recover compromised personal data.

For example, if there is an immediate threat of identity theft or if special category personal data has been published online, [COMPANY] must act without undue delay. This could mean alerting affected individuals even before notifying the ICO (and/or other relevant supervisory authority) of a personal data breach if this would allow affected individuals to take steps to avert an immediate risk such as re-setting access passwords. (See also below – **Does [COMPANY] need to communicate the personal data breach to the affected individuals?**)

Also consider notifying any other third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of reputational harm or financial loss to affected individuals.

Take steps to recover any lost personal data and limit the damage the breach can cause. For example, in addition to the physical recovery of lost equipment, consider using back-up tapes to restore lost or damaged data.

**What must be included in a notification of a personal data breach to the ICO (and/or other relevant supervisory authority)?**

Personal data breaches can be reported to the ICO by telephone on +44 303 123 1113 (normal opening hours are Monday to Friday between 9am and 5.00pm) or online via <https://ico.org.uk/for-organisations/report-a-breach/>. For details of how to report a breach to other relevant supervisory authorities, please check the specific local requirements.

When notifying the ICO (and/or other relevant supervisory authority) of a personal data breach, you must provide the following information:

* the nature of the breach (including, where possible, categories and an approximate number of individuals whose personal data is affected and also the categories and an approximate number of personal data records affected);
* the likely consequences of the personal data breach;
* any measures taken or being proposed by [COMPANY] to address the personal data breach and, where appropriate, mitigate its possible adverse effects;
* name and contact details of [the Data Protection Officer/ *other contact point if there is no Data Protection Officer*].

The above represents the minimum information that must be provided to the ICO (and/or other relevant supervisory authority). However, it may be necessary to provide further details, depending on the circumstances, in order to explain the breach that has occurred. For example, European guidance (which the ICO recognises remains relevant notwithstanding that the UK has left the EU) recommends that you name a third party processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers of data that use the same processor.

The ICO (and/or other relevant supervisory authority) may also ask for additional information as part of its investigation into a breach and you should cooperate with any such requests.

Please keep a written record of any notification that is made to the ICO (and/or other relevant supervisory authority), whether the notification is made in writing or by telephone. Regardless of whether [COMPANY] notifies a personal data breach to the ICO (and/or other relevant supervisory authority), there are record-keeping obligations which must be satisfied for accountability purposes under data protection law. Please see the **Record-keeping** section below.

**What is the time limit for notifying a personal data breach to the ICO (and/or other relevant supervisory authority)?**

Once [COMPANY] is aware of a personal data breach, the breach must - if it is likely to result in a risk to individuals’ rights and freedoms - be notified to the ICO (and/or other relevant supervisory authority) without undue delay and, where feasible, not later than 72 hours after [COMPANY] becomes aware of it.

The 72 hour timeframe does not differentiate between working and non-working hours. If [COMPANY] becomes aware of a personal data breach on a Friday afternoon, the 72 hours would expire on the subsequent Monday afternoon. [COMPANY] has put the following systems in place to facilitate out of hours reporting if necessary: [*insert details, e.g. [Senior Managers/HR/Data Protection Officer/Data Protection Team/Data Protection Lead] will communicate via email to ensure the lead individual has all available information and is able to submit a report to the ICO via their online form.*]

It will usually be clear from the surrounding circumstances when [COMPANY] has become ‘aware’ of a personal data breach (e.g. a third party informs [COMPANY] that it has accidentally received personal data belonging to one of its customers/Employees.)

However, if it appears that a personal data breach *might* have taken place, but it is unclear whether or not it has actually done so, [COMPANY] must immediately conduct a short, initial investigation to establish with a reasonable degree of certainty whether such a breach has, in fact, taken place. For example, if [COMPANY] becomes aware of a rumour that its IT system has been hacked, it should carry out an investigation straight away to check if its system has actually been compromised. Once it has evidence that a hack has occurred, at this point it is ‘aware’ of a personal data breach. The time limit for notification begins to run and a more detailed investigation into the circumstances of the personal data breach can follow.

If it is not possible to provide the ICO (and/or other relevant supervisory authority) with all of the details required (see above **What must be included in a notification of a personal data breach to the ICO (and/or other relevant supervisory authority)?**) or complete the ICO (and/or other relevant supervisory authority)’s online form within the 72-hour timeframe, do NOT delay notification until the remaining information is available. Provide/complete as much of the required information as possible; state clearly the reasons for the delay; and explain that the outstanding information will be provided in phases without undue further delay. As noted above (under **Does [COMPANY] need to notify the personal data breach to the ICO (and/or other relevant supervisory authority)?**), if your subsequent investigation reveals that any risk was contained or mitigated, such that there was no notifiable personal data breach, you should update the ICO (and/or other relevant supervisory authority).

**Does [COMPANY] need to communicate the personal data breach to the affected individuals?**

Data protection law only requires [COMPANY] to communicate a personal data breach to affected individuals where the breach is likely to result in a high risk to the rights and freedoms of individuals.

To help you decide if there is a high risk, carry out the risk assessment set out under **Does [COMPANY] need to notify the personal data breach to the ICO (and/or other relevant supervisory authority)?**above. Although not relevant in every case, the presence of either of the factors below indicates that the personal data breach is very likely to result in a ‘high’ risk:

* the personal data breach involves special category data;
* potential damage is particularly severe (e.g. identity fraud) and communication to affected individuals could allow them to take necessary precautions to minimise likelihood of damage (e.g. changing passwords and notifying banks or other financial institutions, etc).

The scope, context and purposes of processing the personal data will also be relevant to an objective assessment of whether the personal data breach involves a high risk to individuals. For example, unauthorised publication of an individual’s address could cause harm, but if published with a copy of a passport this could expose an individual to a high risk of fraud and identity theft.

[COMPANY] is NOT required to communicate details of a personal data breach to affected individuals where:

* protective measures were already in place to ensure that any personal data would be rendered unintelligible to unauthorised persons (e.g. the personal data was encrypted, the key to decrypt the data has not been compromised and cannot be ascertained by unauthorised persons using available technology. However, bear in mind that if encrypted personal data has been permanently lost without any back-up copy for authorised persons to recover it, this could give rise to a notifiable personal data breach); or
* subsequent measures have been applied to ensure that any high risk to individuals is very unlikely to materialise (e.g. a lost electronic device has been remotely disabled and all data has been deleted); or
* direct communication with the affected individuals would involve disproportionate effort (e.g. where contact details have been lost due to the personal data breach or they were not known in the first place). In this situation, [COMPANY] must consider whether a public communication or similar measure could inform individuals in an equally effective manner.

If you are in any doubt, please consult with the ICO (and/or other relevant supervisory authority). Regardless of whether [COMPANY] communicates the personal data breach to the affected individuals, there are record-keeping obligations which must be satisfied for accountability purposes under data protection law. Please see the **Record-keeping** section below.

**What must be included in a communication of a personal data breach to the affected individuals?**

When communicating details of a personal data breach to affected individuals, you must include the following information:

* the nature of the personal data breach;
* the likely consequences of the personal data breach;
* any measures taken or being proposed by [COMPANY] to address the personal data breach and, where appropriate, mitigate its possible adverse effects; and
* name and contact details of [the Data Protection Officer/ *other contact point if there is no Data Protection Officer*].

You should also, where appropriate, provide specific advice to individuals on how to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

Remember to use clear and plain language and tailor the communication to the particular group of individuals affected (e.g. with translation into a local business language).

Give careful consideration to the best method of contacting affected individuals. Ideally, dedicated messages should be used (e.g. email, SMS, or direct message) but prominent website notification, postal communication, or prominent media advertisements may be necessary, as appropriate. Depending on the circumstances, it may be appropriate to use multiple channels of communication, to maximise the chances of *all* affected individuals receiving the notification. Communications should not be sent with other information such as a newsletter or general update. If you are in any doubt, please consult with the ICO (and/or other relevant supervisory authority).

**What is the time limit for communicating a personal data breach to the affected individuals?**

Once [COMPANY] is aware of a personal data breach, the breach must - if it is likely to result in a high risk to individuals’ rights and freedoms - be notified to the affected individuals without undue delay (i.e. as soon as possible).

Whether [COMPANY] is ‘aware’ of a personal data breach should be determined in the same way as described above in **What is the time limit for notifying a personal data breach to the ICO (and/or other relevant supervisory authority)?**

Given that the purpose of communicating a breach to affected individuals is for the protection of their rights and freedoms, it may be sensible for [COMPANY] to prioritise notifying the individuals, even before making a report to the ICO (and/or other relevant supervisory authority) (provided always that [COMPANY] seeks to comply with the 72-hour timeframe for reporting to the ICO (and/or other relevant supervisory authority)). This could help ensure that the individuals have a better chance of taking action to protect themselves from further security breaches (e.g. by changing affected passwords).

However, when deciding whether to communicate details of a personal data breach to affected individuals, [COMPANY] should always take into account the legitimate interests of any law-enforcement authorities (e.g. the police) where early disclosure could prejudice an investigation. In these circumstances, a delay in communicating a personal data breach to affected individuals may be justified if it is on the advice of the appropriate law enforcement authorities.

**Record-keeping**

Regardless of whether or not a personal data breach needs to be notified to the ICO (and/or other relevant supervisory authority) and/or communicated to affected individuals, [COMPANY] must record the following information in [the Internal Personal Data Breach Register]:

* nature of the breach, including its causes, what took place and the personal data affected;
* effects and consequences of the breach;
* remedial action taken by [COMPANY];
* reasoning for any [COMPANY] decision NOT to notify a breach to the ICO (and/or other relevant supervisory authority) and specifying why [COMPANY] considers that the breach is unlikely to result in a risk to the rights and freedoms of individuals;
* reasoning for any [COMPANY] decision NOT to communicate a personal data breach to affected individuals (e.g. why [COMPANY] considers that the breach is unlikely to result in a *high risk* to the rights and freedoms of individuals, details of protective measures taken or ‘disproportionate effort’ exemption);
* copies of any personal data breach notification to the ICO (and/or other relevant supervisory authority) and, if applicable, communications to affected individuals;
* where a notification or communication of a personal data breach has been delayed, details of the reasons why this delay is justified and not excessive.

**Important:** When completing an entry in [the Internal Personal Data Breach Register], you should seek to ensure that the entry refers to the personal data breach without identifying specific individuals. This is important to safeguard individuals’ privacy and also to ensure that [the Register] itself complies with data protection rules. If you consider that a particular entry in [the Internal Personal Data Breach Register] needs to include information identifying specific individuals in order to provide an appropriate and complete record, you should speak to the [Data Protection Officer/Data Protection Lead/Data Protection Team] for guidance before creating the entry.

**Follow-up procedures**

As with any security incident, [COMPANY] must investigate whether or not the personal data breach was a result of human error or a systemic issue. This investigation should be carried out promptly to see how a recurrence can be prevented (e.g. through better processes, further training or other corrective steps).