Data Breach Reporting Form

Please complete this form to report a personal data breach to the Data Protection Officer.

This form should be read alongside our Data Breach Process document, which provides further information and key definitions.

Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

Report Type:

[ ]Initial report

[ ] Follow-up report

(Follow-up reports only) Legal Office case reference:

About the Breach

What has happened?

Tell us as much as you can about what happened, what went wrong and how it happened

Was the breach caused by a cyber incident?

[ ] Yes

[ ] No [ ]

How did you find out about the breach?

When did you discover the breach?

Date:

Time:

When did the breach happen?

Date:

Time:

Categories of personal data included in the breach (tick all that apply)

[ ]Data revealing racial or ethnic origin

[ ]Political opinions

[ ]Religious or philosophical beliefs

[ ]Trade union membership

[ ]Sex life data

[ ]Sexual orientation data

[ ]Gender reassignment data

[ ]Health data

[ ]Basic personal identifiers, e.g. name, contact details Identification data, e.g. usernames, passwords Economic and financial data, e.g. credit card numbers, bank details

[ ] Official documents, e.g. driving licences

[ ]Location data

[ ]Genetic or biometric data

[ ]Criminal convictions, offences

[ ]Not yet known [ ] Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

[ ]Employees

[ ]Users

[ ]Subscribers

[ ]Students

[ ]Clients

[ ]Patients

[ ]Children

[ ]Vulnerable adults

[ ]Not yet known

[ ]Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

[ ]Very likely

[ ]Likely

[ ]Neutral — neither likely nor unlikely Unlikely

[ ]Very unlikely

[ ]Not yet known

[ ]Please give details

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

[ ]Yes [ ] No

(Cyber incidents only) If you answered yes, please specify (tick all that apply)

[ ]Confidentiality

[ ]Integrity

[ ] Availability

(Cyber incidents only) Impact on the organisation

[ ]High -we have lost the ability to provide all critical services to all users

[ ] Medium — we have lost the ability to provide a critical service to some

[ ] Low -—there is no loss of efficiency, or a low loss of efficiency, and we can still provide all critical services to all users

[ ] Not yet known.

(Cyber incidents only) Recovery time

[ ]Regular — we can predict our recover time, with existing resources

[ ]Supplemented — we can predict our recovery time with additional resources

[ ]Extended — we cannot predict our recovery time, and need extra resources

[ ]Not recoverable — recovery from the incident is not possible, e.g. backups can't be restored Complete — recovery is complete

[ ]Not yet known

Had the staff member involved in this breach received data protection training in the last two years?

Yes

No

Don't know

The breach did not involve a Impact Governance Staff (please give details below):

(Initial reports only) If there has been a delay in reporting this breach, please explain why

(Follow-up reports only) Describe any measures you had in place before the breach with the aim of preventing a breach of this nature

Taking action Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, e.g. confirmed data sent in error has been destroyed, updated passwords, planning information security training.

(Follow-up reports only) Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Have you told data subjects about the breach?

[ ]Yes, we've told affected data subjects

[ ]We're about to, or are in the process of telling data subjects No, they're already aware

[ ]No, but we're planning to

[ ]No, we've decided not to

[ ]We haven't decided yet if we will tell them or not

[ ]Something else (please give details below)

Details of Person making this report, in case we need to contact you for further details:

Name:

Job title:

Email:

Phone:

Please send your completed form to admin@ig-cic.org.uk with ‘Personal data breach notification’ in the subject field.

DATA BREACH PROCESS

The purpose of this document is to outline the process for reporting and managing data breaches. It sets out the requirements of the University to report data breaches to the Information Commissioners Office (ICO) and the action to be taken.

What is a Data Breach?

The ICO defines a personal data breach as 'the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.'

- deliberate or accidental action (or inaction) by a controller or processor; sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen; alteration of personal data without permission; and
- loss of availability of personal data
- A personal data breach occurs when 'any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed'

Reporting a Data Breach

If a data breach has been identified, the Legal Office must be notified immediately, providing the following information:

- What the breach is (e.g. information has been accidentally sent to a third party via email)
- What information is contained/has been breached
- Whose data is involved (e.g. students, staff) and the number of individuals/personal
- data records it concerns
- Where the breach occurred
- When the breach occurred

The likely consequences of the breach Any steps already taken to mitigate the breach (if any)

You can contact the Data Protection Officer at admin@ig-cic.org.uk .

You must report the breach as a matter of urgency as the University is required to report the breach to the ICO no later than 72 hours after the breach occurred.

Steps for reporting a breach, and required timescales

Action required Timescale (from the time the breach is identified) 1 Report the breach to your line manager and the Legal Office immediately

- Complete the Data Breach Reporting Form (available | 90 minutes on in.beds document search) and send to the Legal Office
- The Data Protection Officer will inform the Senior Legal | 2 hours
- Officer, who will then advise the Vice Chancellor and the Registrar
- The Legal Office will then identify whether the 9 hours is required to report the breach to the ICO. This is dependent on the gravity of the breach and the

Discuss the matter with the ICO on a 'without prejudice' basis.

Advise and seek instructions from the Vice Chancellor and Registrar

- If required, the Senior Legal Officer will report the data | 10 hours breach to the ICO keeping within the 72 hour deadline and continue to liaise with them as required.
- The Legal Office will then provide advice and guidance | 13 hours on the steps to be taken to mitigate the breach
- If the breach is considered 'high risk', the Legal Office 16 hours will inform the individuals concerned in conjunction with the relevant department about the breach of their personal data.
- The Legal Office will then record the data breach and 20 hours store all relevant communications on file.
- Informing individuals about a breach of their data

If applicable, the Legal Office will contact the individual/s concerned and notify them of the following:

- The name and contact details of the University's Data Protection Officer

- Adescription of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, if applicable, the measures taken to mitigate any possible adverse effects.

Information to be reported

Any data breach should be reported to the Legal Office, even if it not made directly by staff at the University. This includes information about data breaches made by third parties the University works with, including partners and third party system providers.

These should be reported to the Legal Office as a matter of urgency as above.

Next steps

Once the data breach has been identified and the appropriate action has been taken, the Legal Office will advise on the next steps to be taken and will liaise with you to identify what

updates and improvements are required to ensure the breach doesn't occur again and to reduce the potential of any other data breaches in future.

Legal Office

for marketing purposes, or offer online services to them directly

Process personal data which could result in a risk of physical harm if there is a security breach

Process data in a way which prevents individuals exercising a right or using a service or contract

Participate in a new data-sharing initiative with another organization(s) Transfer personal data outside the EU Process personal data in ways which individuals might not reasonably expect

Also consider doing a DPIA in any major project involving use of personal data, even if it is not sensitive data (e.g. if you are going to use a significant amount of personal data from a large number of data subjects). If you decide not to, document your reasons. Conduct a new DPIA if the nature, scope, context or purposes of the processing changes.

1) If you think it likely that a DPIA is required, contact the Data Protection Officer who can provide guidance, and may ask you to fill in a Data Protection Impact Assessment Form.

Step 2

Determine that the processing is necessary and proportionate

3) Describe the proposed processing and why it is being proposed. This should include an analysis of how the data will be obtained, used and retained.

4) Assess the necessity and proportionality of the processing in relation to the purpose, i.e. can it be done another way that requires less processing of personal data?

5) Always consider whether you can anonymise or at least pseudonymise the data you wish to process. You may be able to anonymise at a later date, safely destroying the original identifiable data. Also consider whether you can conduct the activity with less data either in terms of quantity or quality — only take what you need.

Step 3

Identify the risks associated with the processing

6) Assess the risks to the rights and freedoms of the individuals whose data is being processed, i.e. what would happen if the data was lost or misused in some way? When doing this, you need to consider the rights of individuals under the GDPR. (ICO guidance on rights of data subjects is available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/. If you have any questions about this, consult the Data Protection Officer.

7) Consider the risk that the processing poses (if any) to compliance with the GDPR and to the University more broadly. ws University of Bedfordshire

Legal Office

Step 4 ”

Identify solutions/mitigations to the risks

8) Describe safeguards and security measures put in place, privacy by design, use of data processing and data sharing agreements.

9) Consider seeking the views of the data subjects, or their representatives and other interested parties (i.e. data processors, sector specialists).

Step 5

Feed the results into the proposal

10) Assess if there are changes that need to be made to the proposal, and define how the risks will be monitored.

11) Make sure that the solutions proposed deal with the risk. If you are not sure about acceptable levels please contact the Data Protection Officer.

Step 6 Approval

12) Measures and residual risks should be approved by the relevant project lead. If any residual high risks are identified, the Data Protection Officer should be informed of these (as the ICO may need to be consulted).

13) Once completed, send the DPIA form to the Data Protection Officer, who will review it, and offer advice. It will then be sent for approval to the Senior Legal Officer, and Registrar.

Step 7 Implementation and Review

14) Once the DPIA has been approved, it is safe to proceed. Make sure that all those involved in the processing are aware of the necessary solutions.

15) Keep a record of your processing activities, and regularly review them to ensure they are still compliant with the acceptable position. Be responsive to any necessary changes.

16) Set review dates for 1 month, 3 months, 6 months, and then 12 months after the initial DPIA. Thereafter, review annually or if there is a change in how you process data (whichever is first). Inform the Data Protection Officer of any changes.

Data Protection Impact Assessment Form

“a This form should be filled out at the beginning of any major project involving”

The use of personal data, or if you are making a significant change to an existing process.

Use this form alongside our Data Protection Impact Assessment Guidance, which provides further information and key definitions to help you identify if you need to conduct a DPIA. The final outcomes of your DPIA should be integrated back into your project plan.

Details of Person completing the form:

Name: Job title:

Email:

Phone: DPIA Reference Number (Legal Office to fill): Type:

[] Initial DPIA L] Review (please indicate date of review):

Part A: Identify the need for a DPIA

1. Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Part B: Describe the processing

2. Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

3. Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much

data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

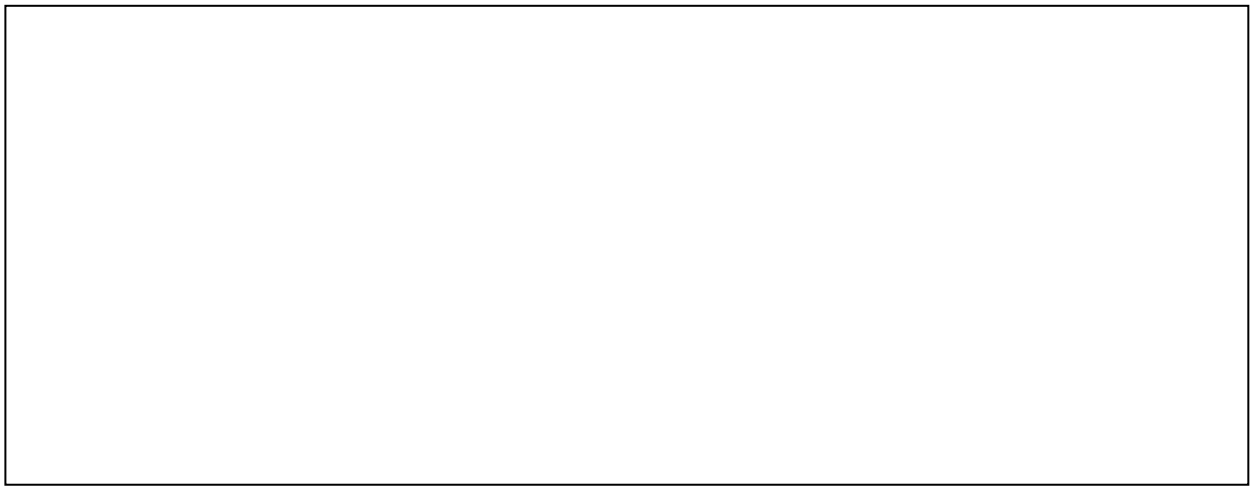
Special category data is personal data which is more sensitive and could create significant risks to a person's fundamental rights and freedoms, e.g. by putting them at risk of unlawful discrimination. Some examples are:

- Race:
- Ethnic origin:
- Politics:
- Religion:
- Trade union membership:
- Genetics; biometrics (where used for ID purposes);
- Health:
- Sex life:
- Sexual orientation:

Criminal offence data is separate from special category data, and means personal data relating to criminal allegations, proceedings, or convictions, or related security measures.

4. **Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?**

5. Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?



Part C: Consultation process

6. **Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views - or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?**

Part D: Assess necessity and proportionality

7. **Describe compliance and proportionality measures, in particular: What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights?**

What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Part E: Identify and assess risks:

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of Harm** (Remote, possible or probable)	**Severity of Harm** (Minimal significant or severe)	**Overall risk** (Low, medium or high)

Part F: Identify measures to reduce risk.

Risk	**Options to reduce or eliminate risk**	**Effect on risk** (eliminated, reduced or accepted)	Residual risk (Low, medium or high)	Measure approved Yes/No

Part G: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks Approved by:		Before accepting any residual high risk, inform

		the DPO, who will consult the ICO.
DPO advice provided:		DPO should advise on compliance, part F measures and whether processing can proceed

Summary of DPO advise:

Senior Legal Officer Approval		Senior Legal Officer to indicate approval, and any further comments/Advice

Comments:

Registrar approval		Registrar to indicate approval, and any further comments/advise.

Comments:

This DPIA will be kept under review by:		The DPO should also review on going compliance with DPIA

Please return your complete form to the Data Protection officer: Legal@ig-cic.org.uk