**Unison Data Protection Breach Report**

The General Data Protection Regulation 2016 (GDPR) defines **personal data** as:

‘*any information relating to an identified or identifiable natural person (‘data subject’) who can be identified, directly or indirectly, by reference to an identifier such as a name, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.’*

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.’*

The GDPR singles out certain types of personal data as likely to be more sensitive and therefore gives them extra protection. These are referred to as **special category data**; and an individual’s trade union membership is one of them.

UNISON processes a great deal of personal data not only for its members, but also its staff and activists. We have several policies and procedures in place to help minimise the likelihood of a data breach occurring, or the severity of the risk should a breach happen.

We understand that most data breaches are the result of human error and/or policies and procedures not being followed. Rarely are they malicious. However, the Information Commissioner’s Office (ICO) can enforce a sanction or fine an organisation for a data breach of up to 20 million Euros or 4% of its global turnover.

Some examples of common data breaches within UNISON are:

* Emails being sent with the recipients address in the ‘To’ or ‘Cc’ field instead of the ‘Bcc’ field (blind carbon copy hides the addresses to all recipients).
* Documents being lost or mislaid i.e. left on a train or in a public place.
* The wrong document being attached to an email i.e. another member’s case file.
* Disposing of personal data insecurely i.e. not using a confidential waste bag or shredder.

Although we are not required to report every data breach to the ICO, we are required under the legislation to keep an internal record of all breaches. It is therefore essential that this report be completed for every data breach.

Once notified, the Data Protection team will consider the likelihood and severity of the risk to people’s rights and freedoms following the breach. If the risk is high, we are required under the legislation to notify the ICO no later than 72 hours after becoming aware of it. Please note, this is *anywhere* within UNISON becoming aware of it, not just the Data Protection team.

If you are unsure what constitutes a data breach, or whether something that has happened needs to be reported, please contact us on [**dataprotection@unison.co.uk**](mailto:dataprotection@unison.co.uk) as soon as possible.

**UNISON Data Protection Breach Report**

|  |
| --- |
| **Date incident occurred** |
|  |
| **Date incident identified** |
|  |
| **Location of data breach** |
| **Branch (include RMS code):**  **Region (include office location):**  **National (include department):** |
| **Name and Position of who committed data breach** |
|  |
| **Have they completed the UNISON GDPR e-learning –**  [**https://e-learning.unison.org.uk/course/view.php?id=42**](https://e-learning.unison.org.uk/course/view.php?id=42) |
|  |

|  |
| --- |
| **What has happened and who has been affected** |
| Please provide as much detail as you can on what has happened, how it occurred and how it was identified. This will enable us to keep a record of data breaches, learn from our mistakes and reduce the possibility of enforcement action from the ICO. |
|  |

|  |
| --- |
| **What personal data has been disclosed** |
| Please provide as much detail as you can about the estimated number of people affected and what data has been disclosed i.e. names, addresses, health condition or if it is a specific document such as a case file. If you don’t know the exact number of people affected, give the most accurate estimate that you can. |
|  |
| **What IT was used** | |
| Please provide as much detail as you can about the IT used. This should include if UNISON systems were used i.e. WARMS or RMS, and if not, what was used to send the communication i.e. Gmail, Outlook etc. This will help identify any additional training requirements. | |
|  | |

|  |
| --- |
| **Summary of action taken** |
| Please detail the action that you have taken so far and any that you plan to take. |
|  |

|  |
| --- |
| **Lessons learned** |
| Please detail what the incident has taught you, for example do you need to make sure that you password protect certain data. You may want to leave this box blank if the breach has not been fully investigated. |
|  |

**Please send the completed form to your regional data protection contact or** [**dataprotection@unison.co.uk**](mailto:dataprotection@unison.co.uk)

|  |
| --- |
| **Regional Data Protection Lead** |
| **Summary of advice provided and any further comments (if any):** |
|  |

|  |
| --- |
| **Data Protection Officer** |
| **Summary of advice provided and any further comments (if any):** |
| **Reported to the ICO:** **Yes/No** (delete as appropriate) |