



Data Breach Policy

Updated: 1st March 2018

1. Scope

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – Notification of a personal data breach to the supervisory authority – and Article 34 – Communication of a personal data breach to the data subject.

The GDPR draws a distinction between a ‘data controller’ and a ‘data processor’ in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

2. Responsibility

- 2.1. All users (whether staff, contractors or temporary staff and third party users) of Wonde Ltd are required to be aware of, and to follow this procedure in the event of a personal data breach.
- 2.2. All staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer (DPO).

3. Procedure – Breach notification data processor to data controller

- 3.1. Wonde Ltd reports any personal data breach or security incident to the data controller without undue delay. These contact details are recorded in the Internal Breach Register. Wonde Ltd provides the controller with all of the details of the breach.
- 3.2. The breach notification is made by email.
- 3.3. A confirmation of receipt of this information is made by email or phone call.

4. Procedure – Breach notification data controller to supervisory authority

- 4.1. Wonde Ltd determines if the supervisory authority need to be notified in the event of a breach.
- 4.2. Wonde Ltd assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting data protection impact assessment against the breach.
- 4.3. If a risk to data subject(s) is likely, Wonde Ltd reports the personal data breach to the ICO without undue delay, and not later than 72 hours.

- 4.4. If the data breach notification to the supervisory authority is not made within 72 hours, Wonde's Data Protection Officer (DPO) submits it electronically with a justification for the delay.
- 4.5. If it is not possible to provide all of the necessary information at the same time Wonde will provide the information in phases without undue further delay.
- 4.6. The following information needs to be provided to the supervisory authority:
 - 4.6.1. A description of the nature of the breach.
 - 4.6.2. The categories of personal data affected.
 - 4.6.3. Approximate number of data subjects affected.
 - 4.6.4. Approximate number of personal data records affected.
 - 4.6.5. Name and contact details of the Data Protection Officer (DPO).
 - 4.6.6. Consequences of the breach.
 - 4.6.7. Any measures taken to address the breach.
 - 4.6.8. Any information relating to the data breach.
- 4.7. In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.
- 4.8. The breach notification is made by electronic means.
- 4.9. A confirmation of receipt of this information is made by email.

5. Procedure – Breach notification data controller to data subject

- 5.1. If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Wonde notifies those/the data subjects affected immediately.
- 5.2. The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 4.6 above.
- 5.3. Wonde takes measures to render the personal data unusable to any person who is not authorised to access it using encryption.
- 5.4. The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.
- 5.5. If the breach affects a high volume of data subjects and personal data records, Wonde makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the Wonde's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.
- 5.6. If Wonde has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Wonde will communicate the data breach to the data subject by email as soon as possible.
- 5.7. Wonde documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.