X-Wrist - Data Breach Policy

1. Introduction

1.1 Under Articles 33 and 34 of the General Data Protection Regulation 2016/679 (**GDPR**), NRG Core Global Limited is required to take prompt action to deal with personal data breaches. Such action includes:

1.1.1 notifying any personal data breach to the Information Commissioner's Office (**ICO**) without undue delay and within 72 hours of having become aware of it (if such breach is likely to result in a risk to the rights and freedoms of individuals); and

1.1.2 communicating details of a personal data breach to the data subject without undue delay (where such personal data breach is likely to result in a high risk to the rights and freedoms of individuals).

1.2 Costin Nita Tanase is the person responsible for the company's compliance with GDPR requirements (**DCC**). His email address is gdpr@x-wrist.com. All discovered or suspected data breaches which come to the attention of any employee, partner or consultant of the company (**Employee**) must be reported to the DCC in accordance with this policy.

1.3 While the consequences of a data breach could be serious for the company, the consequences are likely to be far more serious where a data breach is unreported. It is therefore essential that all Employees become familiar with this policy (particularly paragraphs 1 to 3). By getting the DCC involved at the earliest opportunity, the company dramatically improves its chances of containing and remedying a data breach.

2. What is a personal data breach?

2.1 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of "personal data" (personal data is information relating to and which may identify an individual). In short, there will be a personal data breach whenever 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 and this unavailability has a significant negative effect on individuals.

2.2 Some examples of personal data breaches are the following:

2.2.1 access by an unauthorised third party (whether that unauthorised third party is connected to the company (such as an Employee) or an external third party);

2.2.2 sending personal data to an incorrect recipient (including sending personal data to an incorrect recipient within the company);

2.2.3 devices containing personal data being lost or stolen; and

2.2.4 loss of availability of personal data.

2.3 A personal breach can occur, whether the breach takes place internally or externally.

3. Discovery of a personal data breach: Employees' requirement to report internally

3.1 If any Employee discovers or suspects any personal data breach (irrespective of the likelihood of risk to individuals) (a **Suspected Breach**), that Employee must **immediately** report details of the Suspected Breach in writing to the DCC.

3.2 When reporting a Suspected Breach to the DCC, Employees should, insofar as it is possible at the relevant time, include in their report the information set out in paragraphs 4.2.1 to 4.2.3 (inclusive). Employees should not however delay making a report just because some of this information is not available. Employees are not expected to assess the potential risk to any individual of the data breach: that is a matter to be determined by the DCC.

4. DCC's internal investigation and conclusion

4.1 As soon as possible, but no later than 24 hours after DCC becoming aware of a Suspected Breach, the DCC must conduct an investigation into the facts and circumstances of the Suspected Breach.

4.2 As soon as possible but no later than 48 hours after the DCC becoming aware of a Suspected Breach, the DCC must document the following in writing:

4.2.1 a description of the nature of the personal breach, including where possible, the categories and approximate number of data subjects (individuals) concerned and the categories and approximate number of personal data records;

4.2.2 a description of the likely consequences of the personal data breach; and

4.2.3 a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5. DCC's duty to report

Reporting to the ICO

5.1 If as a consequence of, or at any point during, the internal investigation carried out under paragraph 4 above, the DCC determines that the potential or suspected data breach is **likely to result in a risk** to the rights and freedoms of individuals, the DCC must without undue delay:

5.1.1 notify the personal data breach to the ICO. Such notification to the ICO must include:

5.1.1.1 all of the information set out in paragraphs 4.2.1 to 4.2.3 (inclusive);

5.1.1.2 the name and details of the DCC (or such other point of contact from whom more information can be obtained by the ICO); and

5.1.1.3 details of any further relevant information which the DCC is seeking to obtain, but is not available at the time of making the report to the ICO.

Reporting to the data subject (individual)

5.2 Subject to paragraph 5.3, if as a consequence of, or at any point during, the internal investigation carried out under paragraph 4 above, the DCC determines that the potential or suspected data breach is **likely to result in a high risk** to the rights and freedoms of individuals, the DCC must without undue delay communicate to the data subject (individual) the nature of the personal data breach. Such communication must be in clear and plain language and include, at least, all of the information set out at paragraphs 4.2.1, 4.2.3 and 5.1.1.2 above.

5.3 The DCC is not required to take the steps set out in paragraph 5.2 if any of the following conditions are met:

5.3.1 the company has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

5.3.2 the company has taken subsequent measures which ensure that the risk to the rights and freedoms of data subjects (individuals) referred to in paragraph 5.2 is no longer likely to materialise; or

5.3.3 It would involve disproportionate effort. In such a case, there must instead a public communication or similar measure where the individuals are informed in an equally effective manner.

Examples

5.4 Examples of a potential or suspected data breach which **should** be reported to the ICO if it is likely to result in a risk to the rights and freedoms of individuals include:

5.4.1 personal data of individuals is extracted from a secure website or server controlled by the company, during a cyber-attack;

5.4.2 an email containing personal data is sent to the incorrect recipient;

5.4.3 the company suffers a ransomware attack which results in all data being encrypted, where no back-ups are available and the data cannot be restored, despite there being no presence of malware on the company's systems;

5.4.4 important client information is unavailable for a period of time, following a cyber-attack; and

5.4.5 a direct marketing email is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients.

If there is a **high** risk to the rights and freedoms of individuals, such potential or suspected data breaches should **in addition** be reported to the data subject(s).

5.5 Examples of a potential or suspected data breach which should **not** be reported to the ICO nor to data subject(s) include:

5.5.1 an encrypted CD of the company is stolen during a break-in; and

5.5.2 a brief power outage lasting several minutes means clients are unable to communicate with the company.

6. Documenting of issue – personal data breach register

Irrespective of the whether or not any report is made to the ICO or any communication is made to any individual, the DCC must document any data breach. This must include:

6.1 the facts relating to the personal data breach;

6.2 its effects; and

6.3 the remedial action taken.

7. The company as data controller

This policy has been prepared for situations in which the company is the data controller of personal data. A separate policy will be made available for situations in which the company is acting as a data processor.

8. Penalties for non-compliance

Infringement of the EU GDPR can result in administrative fines of up to 4% of annual global turnover or €20 million – whichever is greater.

Not all GDPR infringements lead to fines. Supervisory authorities such as the ICO (Information Commissioner's Office) have the scope to take a range of other actions, such as:

- issuing warnings and reprimands;
- imposing a temporary or permanent ban on data processing;
- ordering the rectification, restriction or erasure of data; and
- suspending data transfers to third countries.