SPECIAL·UMBRIA

Data breach policy

This policy sets out the policies and procedures of Special Umbria ("SU") with respect to detection of personal data breaches, responding to personal data breaches and notification of personal data breaches to supervisory authorities, data controllers and data subjects.
When dealing with personal data breaches, SU and all personnel must focus on protecting individuals and their personal data, as well as protecting the interests of the SU.

1. Definitions
In this policy:

(a) "appointed person" means the individual primarily responsible for dealing with personal data breaches affecting the SU, being Mr J.J.J. Macco MsC;
(b) "data controller" means the natural or legal person, agency or body which determines the purposes and means of the processing of personal data;
(c) "data processor" means a natural or legal person, public authority agency or other body which processes personal data on behalf of the controller;
(d) "data subject" means an identified or identifiable natural person;
(e) "personal data" means any information relating to a data subject;
(f) "personal data breach" means 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 by SU (including any temporary or permanent loss of control of, or inability to access, personal data); and
(g) "supervisory authority" means the Dutch Authority Personal Data (Nederlandse Autoriteit Persoonsgegevens).

2. Detection of personal data leaks

2.1 SU has put in place technological measures to detect incidents which may result in personal data breaches. As at the date of this policy, these measures include that the server which hosts the SU website monitors and reports anomalous behavior and blocks and reports brute-force attacks. Administrator access to the server is limited to the contractor only.

2.2 SU has put into place organisational measures to detect incidents which may result in personal data breaches. As at the date of this Policy, those measures include:
a. SU permanently deletes all personal data related to a contract within 2 weeks after its expiry and/or fulfillment;
b. staff uses two-factor authentication when accessing data systems containing personal data;
c. staff is regularly trained in recognizing and neutralizing phishing and hacking attempts;
d. internal regulation states that personal data may never be copied, or moved to other systems than the systems where it resides, except for communication with the customer whose data it concerns;

2.3 SU shall regularly review the technical and organisational measures it uses to detect incidents which may result in a personal data breach. Such reviews shall be carried out at least bi-annually.

3. Responding to personal data breaches

3.1 All concerned must notify the appointed person immediately if they become aware of any actual or possible personal data breach.

3.2 The appointed person is primarily responsible for investigating possible and actual personal data breaches and for determining whether any notification obligations apply. Where these obligations apply, the appointed person is responsible for notifying the relevant parties in

accordance with this Policy.

3.3 All personnel must cooperate with the appointed person in relation to the investigation and notification of personal data breaches.

3.4 The appointed person must determine whether SU is acting as a data controller and/or a data processor with respect to each category of personal data that is subject to a data breach.

3.5 The steps to be taken by the appointed person when responding to a breach may include:
(a) ensuring that the breach is as contained as possible;
(b) assessing the level of risk to data subjects as soon as possible;
(c) gathering and collating information from relevant sources;
(d) considering relevant data protection impact assessments;
(e) informing all interested persons within the SU of the breach and the investigation;
(f) assessing the level of risk to SU;
(g) notifying supervisory authorities, data controllers, data subjects and others of the breach in accordance with this Policy.

3.6 The appointed person shall keep a full record of the response of SU to a personal data breach, including the facts relating to the breach, its effects and the remedial action taken. These records will form part of the SU's data breach register.

4. Notification to supervisory authority

4.1 This section applies to personal data breaches affecting personal data with respect to which SU is a data controller.

4.2 SU will notify the supervisory authority of any personal data breach to which this section applies without undue delay and, where feasible, not later than 72 hours after SU becomes aware of the breach, save as set forth in section 4.4.

4.3 Personal data breach notifications to the supervisory authority must be made by the appointed person using the form attached hereto, using secure and confidential means. The appointed person will keep a record of such report in SU's data breach register, including any and all communications on the subject.

4.4 SU will notify the supervisory authority of a personal data breach where it is unlikely to result in a risk to the rights and freedoms of natural persons. The appointed person shall be responsible for determining whether this section applies, and the appointed person will create a record of any decision not to notify the supervisory authority, including the reasons for believing the breach is unlikely to result in a risk to the rights and freedoms of natural persons. This record shall be stored in SU's register.

4.5 To the extent that SU is not able to provide the supervisory authority all the information required (as per the attached form), SU must make all reasonable efforts to ascertain any missing information. The appointed person will keep a record of the reasons for a delayed notification in the register.

5. Notification to data controller

5.1 This section applies to personal data breaches affecting personal data with respect to which SU is the data processor.

5.2 SU will notify affected data controller of any personal data breach to which this section applies without undue delay and where feasible, not later than 72 hours after SU becomes aware of such breach. In addition, SU will comply with the provisions of the contracts with the affected data controllers relating to such notifications.

5.3 Personal data breach notifications to the affected data controllers must be made by the appointed person using the form attached, to be sent to affected data controllers by secure and confidential means. Appointed person will keep records of the notification and any ensuing communication in the data breach register.

5.4 To the extent that SU is unable to provide affected data controllers all information required at the time of initial notification, SU must make all reasonable efforts to ascertain the missing information. That information must be provided to the affected data controllers by the appointed person as and when it becomes available.

6. Notification to data subjects

6.1 This section applies to personal data breaches affecting personal data with respect to which SU is acting as a data controller.

6.2 Notifications to data subject under this section should, where appropriate, be made in consultation with the supervisory authority and in accordance with any guidance given by the supervisory authority with respect to such notifications.

6.3 SU must notify the affected data subjects of any personal data breach to which this section applies if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, except as set forth in section 6.5.

6.4 Personal data breach notifications to affected data subjects must be made by the appointed person in clear and plain language in the form as attached, using appropriate means. The appointed person will keep a record of such notifications and any ensuing communication in the data breach register.

6.5 SU has no obligation to notify the affected data subject of a personal data breach if:

a. SU has implemented appropriate technical and organisational protection measures and these have been applied to the personal data affected;

b. SU has taken subsequent measures which ensure that a high risk to the rights and freedoms of data subjects is no longer likely to materialise;

c. It would involve disproportionate effort (in which case there shall be a public communication or similar measure data subjects are informed in an equally effective manner);

providing that the appointed person shall be responsible for determining whether this subsection applies and create a record of any decision not to notify the affected data subjects. This record should include appointed person's reasons for believing that the breach does not need to be notified to the affected data subjects. This record shall be stored as part of the SU data breach register.

6.6 If SU is not required by this section 6 to notify affected data subjects of a personal data breach, SU may nonetheless do so when the notification is in the interests of SU and/or the affected data subjects.

7. Reviewing and updating this policy

7.1 SU shall be responsible for reviewing and updating this Data Breach Policy.

7.2 This Policy is updated on an ad hoc basis when necessary.

7.3 This Policy is version 1, dated 25 May 2018.

's-Gravenhage (The Hague), the Netherlands / Piegaro (PG), Italy, 1st of January 2022

Notification form

Person responsible for SU data protection:

Description of personal data breach:

Categories of data subjects affected:

Number of data subjects affected:

Categories of personal data concerned:

Number of records concerned:

Likely consequence of breach:

Measures taken to address breach:

Contact details: