Personal Data Breach Incident Response Plan

1.-Definitions

The following terms are used within this document and are defined as shown:

Data subject	An individual who is the subject of personal data, including Customer´s personnel.
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. A data breach is an incident in which personal data has potentially been viewed, stolen or used by an individual unauthorized to do so.
Personal Data	*'*Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controller	Colt
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
The Applicable Data Protection Law	The enforced legislation protecting the fundamental rights and freedom of individuals and, in particular, their

	right to privacy with respect to the processing of personal data applicable in Colt countries.
Technical & Organisational Security Measures	Those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Sensitive Personal Data	*Personal Data that due to its nature its disclosure leads to be considered as* likelihood of serious adverse effects on the protection of personal data, or if it has serious adverse effects on the protection of personal data
Cyber Security Incident Response Team (CSIRT)	A CSIRT is created within an organisation to investigate and assist with recovery from incidents. Within Colt, the CSIRT function shall be owned by Security & Operational Risk Group with the SOC acting as the reporting and coordination point and local business units providing technical and local expertise. Should an incident warrant escalation to the Local Emergency Team or the Colt Crisis Management Team, the appointed Incident Facilitator shall act as the CSIRT representative to that team.
Incident Facilitator	The incident Facilitator is the member of the Colt CSIRT responsible for coordinating Colt's technical response to a cyber-security incident and providing specialist advice to local and senior management. The level of involvement of the facilitator will depend on the scope and seriousness of the incident.

2.-What is a Personal Data Breach

A personal data breach may mean that someone non authorised gets or have access to unauthorised access to personal data. Data breaches can take many forms and can occur by internal or external means including:

- Hackers gaining access to data through a malicious attack;
- Lost, stolen, or temporary misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.);
- Employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.);
- Policy and/or system failure (e.g., a policy that doesn't require multiple overlapping security measures—if backup security measures are absent, failure of a single protective system can leave data vulnerable).

Colt has appropriate policies and technical and organizational measures in place to safeguard and protect your personal data against unlawful or unauthorised access, accidental loss or destruction, damage, unlawful or unauthorised use and disclosure. We will also take all reasonable precautions to ensure that our staff and employees who have access to personal data about you have received adequate training.

However, in case of a Personal Data Breach Incident that can potentially have a range of significant adverse effects on Data Subjects affected including customers personnel, which can result in physical, material, or non-material damage, Colt as data controller has implemented the following process to manage Personal Data Breach Incidents according to article 33 and article 34 of the General Data Protection Regulation (EU) 2016/679 (GDPR), and ensure proper actions required to be compliant with GDPR requirements and Colt´s Binding Corporate Rules.

3. Notification to Individuals affected.

The GDPR requires the Controller to notify a Personal Data Breach Incident to the competent supervisory authority when such Incident is likely to produce a risk of physical, material, or non-material damage **within seventy-two hours** of discovering the breach.

In addition, where there is a likely high risk of these adverse effects occurring, the GDPR requires the Controller to notify the Personal Data Breach Incident to the affected Data Subjects **as soon as is reasonably feasible, and no later than 24 hours**.

Colt is bound to the notification obligations as detailed in the following table:

	Data Controller to communicate a personal data breach incident to data subjects *(Colt is Data Controller)*
Timing	The breach is likely to result in a high risk for the rights and freedoms of data subjects which can result in physical, material, or non-material damage. Individuals affected should be notified without undue delay and no later than 24 hours: the need to mitigate an immediate risk of damage would call for a prompt

	communication on with data subjects as well the need to implement appropriate measures.

4. Communication of a Personal Data Breach Incident to the data subjects.

When the Personal Data Breach Incident is likely to result in a high risk to the rights and freedoms of Data Subjects, Colt shall communicate the Personal Data Breach Incident to the customer without undue delay within 24 hours of becoming aware and having validated the Incident.

The customer shall provide the specific notification means and email where the personal data breach incident shall be notified.

The communication to the Data Subjects shall describe in clear and plain language the nature of the Personal Data Breach Incident and contain the information and measures as follows:

- Describe when possible, the nature of the personal data breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- Name and contact details of Colt´s data protection officer or other contact point where more information can be obtained;
- Likely consequences of the personal data breach;
- Measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication to the Data Subjects shall not be required if any of the following conditions are met:

- The Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach Incident, in particular those that render the Personal Data unintelligible to any person who is not authorised to access it, such as encryption;
- The Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects referred to above is no longer likely to materialise; or
- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

If Colt has not already communicated the Personal Data Breach Incident to the Data Subject, the supervisory authority, having considered the likelihood of the Personal Data Incident resulting in a high risk, may require it to do so or may decide that any of the conditions referred above are met.

In addition, if any personal data breach incident should be reported to Colt, please contact Colt's security incident handler via email at securityincidenthandler@colt.net, by phone:+44 20 7863 5800, including the mandatory information stated in article 33.3 GDPR.

Updated November 2024