Loop Voice and Data
845 The Crescent
Severalls Business Park
Colchester
Essex
CO4 9YQ

Data Breach - Policy

Introductions

Wireless Telecommunications Ltd t/a Loop Voice and Data are required to hold certain information about our clients.

Key information we hold: -

- Contact details, including name, address, telephone numbers and email addresses.
- Payment information
- Details of services with Loop
- Telecommunication System Detail
- Remote details for support

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data breach that could compromise security.

What will we do with personal data?

We will use this data to manage accounts and to support communications equipment that Loop Voice and Data maintain.

From time to time it might be necessary to share this information, for example a third party to help us carry out our duties on your behalf.

How long will we hold data?

We will only keep personal data for as long as we look after client's services.

Purpose

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing a data breach of information.

This policy relates to all data held to enable Loop to provide equipment, support and services to its clients.

This policy applies to all staff, temporary, contractors, consultants, suppliers working for Loop Voice and Data.

The aim of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to prevent further breaches.

Definitions

Data security breaches include both confirmed and suspected incidents.

An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage.

An incident includes but is not redistricted to, the following: -
Loss or theft of confidential or sensitive data or equipment on which such is stored.
Equipment theft
System failure
Unauthorised use of data
Unauthorised disclosure of sensitive or confidential data

Loop Voice and Data
845 The Crescent
Severalls Business Park
Colchester
Essex
CO4 9YQ

Human error
Blagging offences, where information is obtained by deceiving.

Reporting

Any breach must be reported as soon as possible after the incident

The report must have included full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the breach. An Incident Report Form should be completed as part of the process. See (Appendix 1)

All staff should be aware that any breach of Data Protection legislation may result in disciplinary procedures.

Containment

Loop Voice and Data's Data Protection Officer (DPO) will determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

- An initial assessment will be made by the DPO to establish the severity of the breach.
- The DPO will establish what can be done to recover any losses.
- The DPO will establish who will need to be notified and inform the police, where appropriate.
- The DPO will determine what suitable courses of action is to be taken to resolve the situation.

Should you wish to contact Loop Voice and Data's DPO, please email admin@loopvoiceanddata.co.uk

Investigation

The DPO will investigate the breach and access the risks associated with it, for example, the potential adverse consequences for clients and individuals, how serious or substantial those are and how likely they are to occur.

The investigation will take into account the following: -

- The type of data involved
- It's sensitivity
- The protections in place
- What has happened to the data
- Whether the data could be out to any illegal or inappropriate use
- Whether there are wider consequences to the breach

Notification

The DPO, in consultation with relevant colleagues will establish whether the Information's Commissioner's Office will need to notified of the breach, and if so, notify them within 72 hours of becoming aware, where feasible.

Every incident will be assessed on a case by case basis: however, the following will need to be considered:

- Whether the breach is likely to result in a high risk of adversely affecting individual's rights and freedoms under Data protection legislation.
- Whether notifications would assist the individual affected.
- Whether notification would help prevent the unauthorised or unlawful use of personal data.
- Whether there are any legal/contractual notification requirements

Loop Voice and Data
845 The Crescent
Severalls Business Park
Colchester
Essex
CO4 9YQ

- The dangers of notifying. Not every incident warrants notification and over notification may causes disproportionate enquires and work.

Clients whose personal data has been affected by the incident, and where it is considered to be a high risk of adversely affecting the client's rights and freedom, will be informed without undue delay.

The DPO must considerer notifying third parties such as the police, insurers, banks.

A record will be kept of any data breach.

Evaluation

Once the incident is contained, the DPO will carry out a full review of the cause of the breach; the effectiveness of the response and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

Policy Review

This policy will be updated as necessary to reflect best practice and to ensure compliance

May 2018

Loop Voice and Data
845 The Crescent
Severalls Business Park
Colchester
Essex
CO4 9YQ

Appendix 1

Data Breach Reporting Form

Please act promptly to report any data breaches, please notify Loop Voice and Data, Data Protection Officer.

	To be completed person reporting incident
Date incident was discovered	
Date of incident	
Name of person reporting incident	
Contact details of person reporting incident	
Details of incident	
Has any personal data been put as risk	
Description of any action taken	
Received by DPO	
Date	
Forwarded for action to	
Date	