Information Security Policy

Last updated	18th September 2018
Version	1.0

Definitions

GDPR	EU General Data Protection Regulation.
Responsible Person	Individual registered with the ICO as either the Privacy Officer (PO) or data protection officer (DPO)
Register of Systems	means a register of all systems or contexts in which personal data is processed by CCN.
CCN	CCN Communications Ltd and Verevo Ltd
ICO Registration Number	

1. Introduction

CCN Communications Ltd (referred to subsequently as CCN) is committed to processing data in accordance with its responsibilities under GDPR.

Article 5 of GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

GDPR defines personal data as,

- Data that is processed wholly or partly by automated means; or
- The processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
- Can be identified or who are identifiable, directly from the information in question; or
- Who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and may only be processed in more limited circumstances.
- Pseudonymised (the process of altering data in such a way that it can restored to its original state) data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised, then the anonymised data is not subject to the GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.
- Information about companies or public authorities is not personal data.

- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable, and the information relates to them as an individual may constitute personal data.

This policy and any supporting documents describe how CCN adheres to Article 5 of the EU GDPR data protection requirements.

2. General provisions

This policy applies to all personal data processed by CCN.

- The Responsible Person shall take responsibility for CCN's ongoing compliance with this policy.
- This policy shall be reviewed at least annually.
- CCN shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

To ensure its processing of data is lawful, fair and transparent, CCN shall maintain a Register of Systems.

- The Register of Systems shall be reviewed at least annually.
- Individuals have the right to access their personal data and any such requests made to CCN shall be dealt with in a timely manner.

4. Lawful purposes

All data processed by CCN will be conducted on secure systems and only in relevance to the requirement. Data will not be processed unnecessarily and without due care and attention.

- CCN shall note the appropriate lawful basis in the Register of Systems.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in CCN's systems.

5. Data minimisation

CCN shall ensure that personal data are adequate for the purpose, relevant and limited to what is necessary in relation to the purposes for which they are processed. CCN will lonely retain the data that is required for the conduct of its business.

6. Accuracy

CCN shall ensure reasonable efforts are made maintain accuracy in all personal data retained through the full life cycle of the data retention.

All personal data will be maintained for accuracy. Where accuracy cannot be verified, the data will be securely and irrecoverably deleted.

7. Children

CCN does not process any information regarding minors, that is persons under the age of 18.

8. Archiving / removal

To ensure that personal data is kept for no longer than necessary, CCN shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

The archiving policy shall consider what data should/must be retained, for how long, and why.

9. Security

CCN ensures that personal data is stored securely using modern software that is regularly reviewed and updated as and when appropriate.

Access to personal data shall be limited to personnel who need access this information and appropriate security is in place to avoid unauthorised sharing of information.

When personal data is deleted this is done securely in such a way that the data is irrecoverable.

Appropriate back-up and disaster recovery solutions are in place to further secure the data

10. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, CCN shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

CCN will inform the supervisory authority within 72 hours of it becoming aware of a breach that has compromised personal data.

If the breach is likely to result in a high risk of adversely affecting individual's rights and freedoms, these individuals will be informed as soon as possible.

A record will be maintained of all breaches, irrespective of whether they require reporting to the ICO.

Appendixes

Appendixes

Register of Systems

Name of system	Purpose	Supporting entity (3rd party hosting company or supported internally)	Contact details of supporting entity
TMS Analysis	Driver Licence Management	TMS Analysis Online	Christine@tmsanalysis.co.uk
Payroll	Payroll	Taylor Cocks	payroll@taylorcocks.co.uk

Breathe HR	Human Resources	Breathe HR	Ashley Adams
Freshdesk	Claims Management	Freshdesk	Lucy Alexander

END OF POLICY