Crick Woodlands
A community growing together
Registered Charity Number : 1090645

CRICK Woodlands

General Data Protection (GDPR) Guidance Policy

Background to GDPR

Data Protection laws arose from concerns over individuals' right to privacy as increasing amounts of personal information was gathered by businesses and other organisations throughout the 20th century.

Digital technology has changed the way many organisations operate and the evolving means of collecting, storing and processing personal data has meant that laws have needed to be significantly changed to keep pace. GDPR takes account of modern methods of capturing and processing people's data and takes steps to ensure individuals have sufficient control over their information.

It is important to remember though, that data protection isn't just about digital information but all personal information, including that which is recorded or stored in paper copies.

GDPR details procedures that are required by law, so Crick Woodlands needs to adhere to these to be compliant and avoid breaches, fines from the Information Commissioner's Office and, potentially, a compensation claim on behalf of those individuals affected. It is therefore essential to make sure that we are following best practice in terms of the following:

- How we gather information
- How securely we store information
- How we comply with reasonable requests for the information we hold
- How we can evidence any of the above in the event of an audit

Ensuring that we have clear policies and acceptable processes in place will give us a strong case against a hefty fine in the event of a breach or audit.

Types of data

- **Personal Data**
  This is any information which relates directly to an individual and can be linked directly to them. For example, this includes: name, phone number, email address, photographs and economic data. This kind of data is the focus of GDPR and data protection.
- **Anonymous Data**
  Data which has been anonymised properly cannot be traced back to the original individuals in any way but can still be processed by organisations to conduct research. Fully anonymous data is not covered by GDPR as it contains no personal information to protect.
- **Pseudonymous Data**
  Some data, which has been properly pseudonymised, can only be connected back to an individual using a specific 'key' or code. This can be an extra layer of security but the data is still treated as Personal Data under GDPR because of the possibility of personal identification.

Principles of GDPR

- **Lawfulness, fairness and transparency**

This covers the primary areas of concern that data should be gathered and used in a way that is legal, fair and understandable. The public have the right to know what is being gathered and have this corrected or removed.

- **Purpose limitation**
  We should only use data for a legitimate purpose specified at the time of collection. This data should not be shared with third parties without permission.
- **Data minimisation**
  The data collected by us should be limited only to what is required for the purpose stated. We should not collect data en masse without purpose.
- **Accuracy**
  The personal data we hold should be accurate, kept up to date, and, if it is no longer accurate, should be rectified or erased.
- **Storage limitation**
  Personal data should only be stored for as long as is necessary. Data can be archived securely and used for research purposes in the future. Where possible, the personally identifiable information should be removed to leave anonymous data.
- **Integrity and confidentiality**
  Personal data should be held in a safe and secure way that takes reasonable steps to ensure the security of this information and avoid accidental loss, misuse or destruction.

Crick Woodlands GDPR Policy

We will consider the following points about personal information we hold:

- Should we be collecting this?
- Is this useful and accurate?
- Have we got clear permission or valid justification to use this?
- Should we still be holding this?
- Is our data held securely and safely? Is this request from the individual concerned?
- Are the businesses we work with also compliant?

Audit

We will undertake a full audit of the data we hold; this includes paper and digital records.
Once we've gathered and assessed all the personal information we hold, we will decide whether it is still needed, if not, it will be deleted. For the data we would like to retain, we will need to be able to demonstrate valid reasons or reasonable consent from the individuals to do so.
Most management tasks, such as administering membership or other activities people would reasonably expect, could be classed as 'legitimate interests' but other communications, outside our core activities may rely on 'consent' as our condition.
Under GDPR, consent from individuals must be affirmative, freely given, specific, informed and unambiguous. This means that they must actively give consent for their data to be processed. Silence, inaction and pre-ticked boxes are not valid as consent. A record of how and when consent was granted should be kept on file.

Privacy statement

A clear, simple privacy statement will be available on our website. This will include the information we are required to provide:

- The identity of the Data Controller
- The purpose of collection
- Whether any sharing with third parties or international transfers will take place
- How long the data will be held
- Details of the individual's rights regarding the data

Reference to this statement should be included in any communications with individuals, along with the option to opt-out.

Retention policy

Any data we hold will only be kept for as long as it is necessary and useful. We will review all our data every two years to refresh the data and keep only what is relevant and current. Data will always be deleted if an individual has withdrawn consent, or if the data is no longer up to date. Certain elements of the data can be held indefinitely if these are anonymised (removing personally identifiable data).

Rights and requests

- **Right to be informed**
  Individuals will be informed of how their data is collected, stored and processed in a clear, accessible way. This will be provided in our Privacy Statement and by request.
- **Right of access**
  Individuals can request access to a copy of their data in electronic form and details of how it is processed. We will provide this, for free, within one month.
- **Right to rectification**
  Individuals are entitled to have their data corrected if it is inaccurate or incomplete. We will do this within one month, or two if it is a particularly complex task.
- **Right to erasure**
  This permits individuals to request the deletion of their data; We will do this within one month, unless we have a strong, valid reason.
- **Right to restrict processing**
  Individuals can request a halt on processing if they object to accuracy or purpose but we can still hold the data until resolved. There will be an immediate pause in the processing.
- **Right to data portability**
  Individuals can request their data in a suitable digital format, sent directly to them or to a third party. We will do this within a month, or two if it is a particularly complex task.

Right to object
Individuals can, in certain cases, object to the processing of their data, eg. in direct marketing. We will provide reasonable means to object and act on this within one month.

Points to Note : Special categories

These categories of personal data have stricter rules regarding their processing, so must be treated carefully. They can be processed *only* with explicit consent to do so, or if it is a necessity in performing a contract. This type of information can, however, be gathered in an anonymised form for the purpose of research and monitoring.

- Racial and ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Data on health, sex life or sexual orientation
- Genetic or biometric data

Children
GDPR enhances the protection of children's personal data. Any privacy notices for services offered directly to a child must be written in clear, simple language to be taken as valid. A child under 16 cannot give consent themselves. This is required from a person holding 'parental responsibility'.

International transfers

Cloud storage and other online services may be based internationally and storing their data outside the EU. We must ensure that any third-party services we use are compliant with GDPR.
Many large tech companies (e,g. Google, Dropbox) have bases within the EU so that they can work within Europe and easily store and process data under GDPR. However, other websites and cloud storage services may

be entirely based in the United States or elsewhere and store data in another jurisdiction; these sites should not be used.