UDOIT Data Protection GDPR Policy

UDOIT is fully committed to comply with the General Data Protection Regulation (GDPR). The GDPR applies to all organisations that process data relating to their employees, as well as to others including customers, contractors and clients. It sets out principles, which should be followed by those who process data; it gives new and extended rights to those whose data is being processed.

To this end, UDOIT endorses fully and adheres to the six principles of data protection, as set out in the Article 5 of the GDPR.

1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Data must be 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.
5. Data must be 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.
6. Data must be 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.

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the UDOIT will:

- observe fully the conditions regarding the fair collection and use of information including the giving of consent.
- meet its legal obligations to specify the purposes for which information is used.
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements.
- ensure the quality of information used.
- ensure that the information is held for no longer than is necessary.
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect).

- take appropriate technical and organisational security measures to safeguard personal information.
- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection.
- ensure that personal information is not transferred abroad without suitable safeguards.

Adherence will be achieved through application of the 'UDOIT GDPR Compliance Implementation Policy'.

Designated Data Protection Officer

The Designated Data Protection Officer (DPO) will deal with day-to-day matters. Any member of staff, or other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the DPO. Details of the current designated DPO can be found on UDOITs website.

Status of this Policy

The Policy does not form part of the formal contract of employment for staff but it is a condition of employment that staff will abide by the rules and policies made by UDOIT from time to time. Any failure to follow the Data Protection Policy may lead, therefore, to disciplinary proceedings.

Staff Responsibilities

All staff are responsible for:

- checking that any information that they provide to the organisation in connection with their employment is accurate and up to date.
- informing the organisation of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The organisation cannot be held responsible for any errors unless the employee has informed it of such changes.

Data Security

All staff are responsible for ensuring that:

- any personal data that they hold is kept securely.
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Disaster Recovery

1. Back ups are made regularly, at least weekly, to storage devices.
2. Firewalls and virus checkers are kept up to date and running, and users are trained in virus avoidance and detection.
3. Computers are protected from physical harm, theft or damage.
4. The organisation plans for how to deal with loss of electricity. It uses paper forms where necessary for temporary record keeping.

Subject Consent

The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed. As required by the GDPR, the organisation takes a "granular" approach i.e. it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, the organisation ensures that people can easily withdraw consent (and tells them how this can be done).

Conclusion

This policy sets out UDOIT's commitment to protecting personal data and how that commitment is implemented in respect of the collection and use of personal data.

Signed:_____

UDOIT Chair, on behalf of the Trustees

Date: _____

Policy review date: _____

Source URL: https://app.croneri.co.uk/topics/data-protection-gdpr-policy