Daylight Norfolk Company

General Data Protection Regulation Policy

Adopted: 27th May 2018
To be reviewed annually. Date of next review: May 2019

Purpose of the policy and background to the General Data Protection Regulation

This policy explains to clients, customers, staff and the suppliers about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement. This policy explains the duties and responsibilities of Daylight Norfolk Company (the company) and it identifies the means by which the council will meet its obligations.

Identifying the roles and minimising risk

GDPR requires that everyone within the company must understand the implications of GDPR and that roles and duties must be assigned. GDRP requires the appointment of a Data Protection Officer (DPO) if the organisation deals with CCTV or large scale "special categories" of personal data. Our company does not by law require a DPO.
GDPR requires continued care by everyone within the company and its staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the company facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as high / medium risk to the company. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the company undertaking training in data protection awareness.

Data breaches

One of the duties assigned to the DPO is the investigation of any breaches. Personal data breaches should be reported to the DPO for investigation. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days of being made aware) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.
It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, to use IT in any way that may cause problems for the company, for example the discussion of internal company matters on social media sites could result in reputational damage for the company and to individuals.
The company currently utilises Facebook, Twitter and Instagram alongside its website, and only Mr M Caton will have access to these applications, and post information to, these sites.

Privacy Notices

Being transparent and providing accessible information to individuals about how the company uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what Daylight Norfolk Company does with their personal information. A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the company. Daylight Norfolk Company will

adopt a privacy notice to use, although some changes could be needed depending on the situation. All privacy notices must be verifiable.

Information Audit

The DPO must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the company will share that information with. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the company undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

Individuals' Rights

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, then the DPO must respond to this request within a month.

If a request is considered to be manifestly unfounded then the request could be refused.

Summary

The main actions arising from this policy are:

- Daylight Norfolk Company must be registered with the ICO.
- A copy of this policy will be available on the company's website. The policy will be considered as a core policy for the company.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.
All company representatives and employees are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of Daylight Norfolk Company