

GDPR Update report to P&R Committee January 2019

Appointment of External Company to provide GDPR services

A quote was obtained in July 2018 from a company offering GDPR services which included:

- Undertaking a full data audit
- Submitting a data audit report
- Providing template policies
- Providing template documents

Also offered were a DPO (Data Protection Officer) service (annually renewable), including training provision, ongoing compliance monitoring, a data protection impact assessment advice service (separate charge), a remote computer audit (remote off-site audit charged per pc) and IT solutions.

(The confidential quote with full detail is available for members in their packs.)

Note: the appointment of a DPO is not a legislative requirement.

Comments

Since the quote was obtained a considerable amount of work has been put into ensuring the Council complies with the new regulations with the assistance of advice from the website of the ICO, NALC, SLCC and CALC. The SLCC website has been a particularly useful source for templates whilst the clear, user-friendly guidance from the ICO website has been invaluable.

A recording of the Cornwall Council training session given by Simon Mansell for their members was made available to all STC members and staff and will be used for an additional training session to be held shortly.

Essential policies and documentation have been established.

Procedures have been established for recording processing activity related to personal data including breach reporting.

The IT system has been reviewed and upgraded to ensure security compliance.

Current Status

It has not been possible for the responsible member of staff to be given the time to fully complete the necessary work on this important area. There should also be time allowed for ongoing monitoring.

A draft data audit has been done but needs to be finalised alongside compliance checks with individual members of staff. (Outstanding area – admin staff.)

Privacy notices for some areas of business have to be put in place – templates can be readily sourced from the SLCC.

An internal review of compliance and associated activity, including whether procedures require any amendments, is likely to be a worthwhile exercise at this stage.

An additional training session for newly appointed staff, members and NP members is to be run on 5th February (daytime), at a later date an evening session is to be held for members who are unable to attend in the daytime.

It has not been established who would undertake the work of a DPO in the event of a data breach although the current first point of contact is the SP&DC Officer.

Should the Council appoint the external service provider?

A lot of the areas offered as part of the service have already been done. GDPR awareness is good and whilst there is still work to do (see above) the Council is working in a compliant manner.

Ongoing advice: The Council has access to a number of advice providers including the SLCC, CALC and NALC. The ICO website is regularly updated and is currently publishing guidance that combines previous GDPR advice with the new Data Protection Act 2018. The monthly e-bulletins provide summaries of the newly published material and is used to monitor any updates.

Whilst the external service provider offers ongoing advice, a member of staff will still have to do any associated work that arises from the advice.

Data Protection Officer: this is not a legislative requirement but would have value in the event of a data breach.

There is no requirement for the services relating to IT as the system put in place recently was tailored to ensure compliance with the new data protection regulations.

Other factors:

The library is due to be taken on shortly. There will need to be an audit undertaken and it will need to be established who is responsible for some areas as data controller and potentially as data processors. The audit has been provisionally booked for 12.03.2019 with any resulting implications to be reviewed following this visit.

Changes in staffing structure and responsibilities may have altered some of the audit details previously recorded.

Estimated time required to fully complete outstanding work on GDPR is approximately one month. It is suggested that once this work is completed an external auditor (to be appointed) works with the responsible member of staff to check for compliance.

Mandy Thomas
Senior Policy and Data Compliance Officer