Audit, Risk and Governance Committee
Meeting to be held on Monday, 29 October 2018

Electoral Division affected:
(All Divisions);

General Data Protection Regulation Update

Contact for further information:
Paul Bond, Tel: (01772) 534676, Head of Legal and Democratic Services
paul.bond@lancashire.gov.uk

Executive Summary

The report provides an update on the implementation of controls to ensure compliance with new data protection legislation across the authority.

Recommendation

The Audit, Risk and Governance Committee is asked to note the report.

1. Background

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) came into force in the UK on 25 May 2018. The legislation makes provision for the processing of personal data. Personal data means any information relating to an identifiable living individual.

Data protection principles

Six data protection principles (rules) for processing personal data came into force, they said that personal data must be:

1. Processed lawfully, fairly and in a transparent manner (we must have a legal basis for processing and tell the data subject what we are doing with their data via a privacy notice).
2. Processed for specified, explicit and legitimate purposes (we can't collect it for one reason and use it for another).
3. Adequate, relevant and limited to the purposes for which we collected it (we can't collect more than we need).
4. Accurate and up to data (we have to ensure data quality).
5. Not kept longer than is necessary (we need to set data retention periods).
6. Processed in a manner that ensures security (we need to use technical and organisational controls to ensure the security of personal data).

Lawful reasons for processing personal data

The first principle (processed lawfully) means we need to satisfy one of the following lawful reasons for processing personal data:

- Consent of a data subject (positive affirmation of consent).
- Processing is necessary for the performance of a contract with the data subject (e.g. employment contract).
- Processing is necessary for compliance with a legal obligation (e.g. The Care Act).
- Processing is necessary to protect the vital interests of the data subject or another person (to protect someone's life).
- Processing is necessary for the performance of a task carried out in the public interest (public health purposes or social protection but based in law).

There are also extra restrictions on processing more sensitive personal data such as health data and crime data.

Personal data breaches

The sixth principle covers security. If we are responsible for a personal data breach leading to the unauthorised disclosure of personal data we could be heavily fined by the Information Commissioner's Office and the data subject would have the right to claim compensation if they have suffered a risk to their risks or freedoms.

New rights

The legislation has given people a new set of 'rights'…

- The right to be informed of what we do with their personal data - via Privacy Notices.
- The right of access to their personal data - via Subject Access Requests (SARs), the timescale for response has been reduced from 40 calendar days to one calendar month.
- The right of rectification - inaccurate or incomplete data must be rectified within one month.
- The right to erasure - individuals have a right to have their personal data erased and to prevent processing unless we have a legal obligation to do so.
- The right to restrict processing - individuals have the right to suppress processing. We can retain just enough information about the individual to ensure that the restriction is respected in future.
- The right to data portability - we need to provide individuals with their personal data in a structured, commonly used, machine readable form when asked.
- The right to object - individuals can object to their personal data being used for profiling, direct marketing or research purposes.
- Rights in relation to automated decision making and profiling - the GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Information sharing and privacy

We must now include GDPR in all our contracts where personal data is processed and we must have:

- Information sharing agreements with our partners where we are joint data controllers.
- Privacy notices to give out and put on the Internet to tell people what we are doing with their personal data.
- Privacy impact assessments at the start of any project where personal data is to be processed so as to risk assess the project against legislation compliance.

Fines

If we do not comply with the legislation, the Information Commissioner's Office can issue the county council with an:

- Information notice asking for information about our processing.
- Assessment notice saying an assessment by the Information Commissioner's Office will take place.
- Enforcement notice ordering us to take or refrain from certain actions including the erasure of data.
- Penalty notice for the infringement of data protection of up to 20 million euros or 4% of turnover.

One of the biggest changes in the legislation is that the council must keep evidence of our compliance.

2. What the County Council have done to comply with the new legislation

Preparations for GDPR and DPA 2018 began at the start of 2017 with the Information Governance Team systematically assessing each part of the legislation and putting controls and processes in place to ensure the authority would be compliant when the legislation came into force on 25 May 2018.

The following actions have been taken:

Governance arrangements

- The responsibilities of the Senior Information Risk Owner (SIRO) and the Data Protection Officer (DPO) have been assigned to senior members of staff.
- The Corporate Information Governance Group (CIGG) meets once a quarter to ensure that the council is compliant with all data protection legislation. The group is chaired by the Information Governance Manager and includes key senior officers across the authority who have responsibilities for data protection.
- A dedicated security manager investigates all information security incidents. All council staff have a mechanism for reporting information security incidents.

This facility is also available on the council website for service users, partners and suppliers to report information security incidents.
- A dedicated assurance manager satisfies the new 'accountability principle' through spot checks, audits and performance statistics.

Requests for help

- In 2017 the Information Governance Team dealt with **4,050** registered requests for help or action in connection with data protection.
- In 2018 (to 1 October 2018) the Information Governance Team has dealt with **9,484** registered requests for help or action in connection with data protection. This gives a projected increase for the year of 200%.

Awareness and advice

- A presentation has been given to all services across the council and has been made available on the Intranet.
- The mandatory annual information governance eLearning course has been updated to include the new data protection legislation and has been completed by 76% of all staff. Staff who do not have access to the network have been given a hard copy.
- Specialist training including face to face and eLearning training has been undertaken by all staff working closely with GDPR, including the council's SIRO, the DPO and all members of the Information Governance Team. All are now registered GDPR Practitioners.
- Bite sized briefings and bespoke advice has been given to all Councillors.
- A compliance letter has been made available for all services should they need to show compliance.
- All schools in Lancashire have had access to bespoke face to face training organised by the council and a school pack of templates and advice has been made available on the schools portal. General specialist advice has also been given to all schools requesting help.
- Specialist advice has also been given to care homes to help them comply with the new data protection legislation.
- Staff notices and team talk articles and the Chief Executive's blog have all regularly updated staff on the new legislation.
- A large Intranet web site comprising help and advice regarding the new legislation is available for all network users, alongside hard copy advice for non-network users. The advice is comprehensive and covers all relevant areas and includes a 'top tips' and a 'question and answer' section. Advice and guidance published in the 'raising awareness' section includes the GDPR staff presentation, a quick guide, implications for councillors and advice on consent and contracts. There is also a standard letter that can be adapted to show how services comply with GDPR and the DPA 2018.

Record of all personal data processing

- The Information Governance Team conducted an internal audit of all personal data being processed across the council. This was done in conjunction with

Heads of Service and Information Governance champions. The audit record shows the purpose for processing, who the data is shared with, how long we keep the data, the security measures used to protect the data and the legal basis for processing the data.
- Where consent is the legal basis for processing the audit records show where the evidence of consent is held.

Legal contracts, policies and sharing agreements

- Existing contracts are in the process of being varied to meet the GDPR requirements. This is a very time-consuming task. Revised contract clauses have been prepared for inclusion in new contracts. Where the lawful basis for processing is consent, standard consent letters have been created and distributed.
- Advice has been given regarding hundreds of projects dealing with personal data, privacy impact assessments have been completed and saved with the project documentation.
- A general privacy notice and multiple service specific privacy notices have been created and published on the Internet and given out to service users, showing them how their personal data is being handled in line with the new legislation. The notices detail all personal data processing, information sharing, people's rights and retention periods, and how to exercise their new rights.
- A system to deal with requests in regard to these new rights has been created. This includes the 'right of access' where the statutory response time for SARs has been reduced from 40 calendar days to 1 calendar month.
- An award winning information sharing gateway has been created to allow organisations sharing data (joint data controllers) to do so electronically and within the parameters of the legislation via information sharing agreements. To date there are 383 organisations using the gateway to share data with the council, with all data flows being listed and signed off by senior officers.
- Regular meetings take place with the council's major partners and suppliers, including BTLS (ICT) and LPP (Pensions) to ensure compliance with the legislation.
- All 19 IG policies were reviewed and updated in early 2018 to reflect the introduction of GDPR, including policies on security, information handling, access controls, and internet, email and telephone use. The policies were subsequently approved by CIGG in February 2018 as part of the annual review of the information governance framework and policies.

Security

- The council has a dedicated officer who manages and investigates all information security incidents and liaises with the Information Commissioner's Office regarding any breaches of the legislation that occur. To date the council has never been fined and this is purely down to the number of controls in place at the council.
- All reportable data breaches, are reported to the Information Commissioner's Office within 72 hours of us becoming aware of them as required by the

legislation. Breaches are reportable if they pose a risk to a person's rights and freedoms.

- The information Security Incident Management Policy sets out the types of incident and how these are to be reported and investigated. The policy describes the action required to ensure that breaches are responded to appropriately, including an online incident report form which is delivered electronically to the SIRO, DPO and the Information Governance Team.
- The Senior Information Security Officer investigates all incidents and completes an Information Security Incident Risk Assessment. Incidents of personal data sent to the wrong person are reported to the Corporate Management Team in a quarterly dashboard and evidence relating to the investigation is recorded on the Information Governance Team's case management system.
- The number of information security breaches reported to the Information Commissioner's Office in 2017 was 6 of 185 incidents and up to Q3 in 2018, 9 of 258 incidents. This information is reported on the Information Governance intranet site and to CIGG. The reason for the increase is due to the increase in awareness across the authority of the need to report incidents that could be possible breaches of the legislation.
- The Information Governance Team's risk register was updated in 2018 to reflect the introduction of GDPR, and is reviewed quarterly in line with corporate risk management requirements. The Corporate Risk and Opportunity Register includes an information security risk and identifies additional controls introduced to comply with GDPR.
- BTLS manages the technical security of the network and pass any requests in connection with the legislation through to the Information Governance team for approval.

Internal audit report

- In September 2018 the Internal Audit service carried out an audit into the council's compliance with GDPR and the Data Protection Act 2018. The audit gave the council 'Substantial Assurance' and zero actions to complete.
- The internal audit report concluded:

    - *Overall, we can provide **substantial** assurance over the arrangements put in place by the council to ensure the council's information governance (IG) strategy, policies and procedures are GPDR compliant. A new IG framework allocates data protection roles and responsibilities, lists IG policies and records improvement actions. Officers and members have been made aware of the changes in the law through publication of updated policies and training. Data processing audits were performed to assess the implications of GDPR on services, including the lawful basis for processing data, and privacy notices and procedures for obtaining consent were subsequently updated.*

Consultations

N/A

Implications:

N/A

Risk management

The risks of not complying with the new data protection legislation include:

- Fines of up to £17.7 million (20 million euros)
- Damage to the reputation of the council
- Risks to the rights and freedoms of the council's staff and service users

Local Government (Access to Information) Act 1985
List of Background Papers

Paper	Date	Contact/Tel

None

Reason for inclusion in Part II, if appropriate

N/A