GENERAL DATA PROTECTION REGULATIONS (GDPR)

Applicable from 25 May 2018

Table of Contents

GDPR at a glance

The GDPR are EU generated regulations that reinforce existing UK Data Protection laws and will be enacted into UK law. The Regulations apply from 25 May 2018 and its impact affects most areas of UK data protection law. Compliance with the GDPR is demonstrated in the policies and procedures applied by AELP.

The following infographic shows the different elements of the regulations.

AELP GDPR Policies

The Regulations are covered by the following five policy areas:

1. Information governance policy
2. Information management policy
3. Archiving policy including Retention and Disposal
4. Data privacy policy
5. Data breach and incident management

1. **Information Governance Policy:** the overarching policy explaining the governance process on roles and data, and principles of data protection.

   The policy applies to all AELP personnel who create, store, share and dispose of information. It sets out the procedures for sharing information with stakeholders, partners and suppliers, and concerns the management of all paper and electronic information and associated systems within the organisation, as well as information held outside the organisation that affects its regulatory and legal obligations.

   The AELP policy meets the GDPR effective from 25 May 2018 by demonstrating that technical and organisational policies and practices are applied to the "legal" bases for processing data. These are:

   i. Legal requirement
   ii. Contractual agreement
   iii. Agreement by consent
   iv. Public interest
   v. Incorporated within the policies and procedures are the eight principles of Data Protection

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means that consent is insufficient: the individual must be informed of exactly what their data is being used for. Furthermore, organisations must inform the individual of their right to withdraw consent at any time.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date. This means that the organisation should not rely on individuals to update their information, but they should be proactive to ensure personal data is current.

Storage limitation	Personal data shall 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.
Integrity and confidentiality	Personal data shall 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. Customers can also request to see the information held on them by submitting a subject access request and can also request that any data held is transferred to another organisation.
Accountability	The controller shall be responsible for, and be able to demonstrate, compliance with the GDPR.
Data Transfer outside EU	Data should not be transferred to other countries that do not have the same level of Data Protection.

2. **Information Management Policy:** this sets out how the organisation and its employees manage and work with personal data.

   AELP has nominated the Director of Finance as the Data Controller whose role is to ensure that AELP complies with the GDPR and maintains the registration requirements of the Information Commissioners Office (ICO).

   AELP maintains records to indicate processing activities, data sharing and retention. All data held is mapped to specific areas of the business and is kept either in paper form, electronically or both. Annual reviews are carried out to ensure:

   - Information access is restricted and use is monitored
   - It complies with regulations
   - It is secure, and the security policy and procedures are effective
   - The IT infrastructure and performance where data is held are robust
   - Risk assessments are included and reviewed within the Company's Risk Register

   AELP is not required by the Regulations to formally appoint a Data Protection Officer but has nominated employees from across the business to maintain and report changes in data processing, including fielding all data requests.

3. **Archiving policy including Retention and Disposal:** this supports AELP's accountability through the proper retention of records and that disposal decisions are taken with proper authority.

   AELP creates and holds a wide range of recorded information. Data needs to be properly retained to enable AELP to meet its business needs and legal requirements.

   The permanent retention of records is undesirable and disposal is necessary to free up storage space,

reduce the administrative burden and to ensure that AELP does not unlawfully retain records for longer than necessary (particularly those containing personal data).

The policy covers the records listed below:

- Paper documentation
- electronic files (including databases; Word documents; PowerPoint presentations; Excel spreadsheets; webpages and e-mails)
- photographs; scanned images; CD-ROMs, video tapes, memory sticks and backup drives
- AELP Specific Records

3.1. Retention Schedules

Regulatory Operations/Governance

Description	Disposal Period
Annual audited reports and accounts	10 years
Board packs	6 years
Risk registers	3 years after register is superseded
Board meeting minutes	6 years

Policy, Strategy and Public Affairs

Description	Disposal Period
Model contract	3 years after contract is superseded
MP briefings	3 years
Memorandums of Understanding with public bodies	3 years after MOU ends

Human Resources

Description	Disposal Period
AELP Organisation chart	When superseded
Policies and procedures related to the recruitment and employment of staff	When superseded
Pay and Grading Framework and related documents	When superseded
Performance management framework	When superseded

Internal Financial Information

Description	Disposal Period
Annual budgets	6 years
Monthly management accounts	6 years
Expenditure control procedure	Until superseded
Expenses claim procedure	Until superseded
Investment records	2 years
Asset registers	6 years after item/asset is disposed of
Supplier invoices	6 years
Employee Expense claims	6 years

Bank Account Details – Cheques and Associated Records

Description	Disposal Period
Cheque book/butts for all accounts	2 years
Bank deposit books / slips / butts	2 years
Bank statements, periodic reconciliations	6 years plus current year
Electronic banking and electronic funds transfer – Cash transactions; payment instructions; deposits; withdrawals	Disposal action in line with investment records

Accounting system

Description	Disposal Period
All accounting data	Minimum 6 years
Journals	6 years
Year-end file, reconciliations and variations to support ledger balances and published accounts	6 years

Salaries and Related Records

Description	Disposal Period
Employee salaries monthly	6 years
PAYE reports	6 years

SMP, SSP and SPP papers	6 years
Pension documentation	6 years

Contract Records

Description	Disposal Period
Signed contracts from customers	3 years after completion of contract
List of approved suppliers	An active document – updated regularly
Lease Agreement	2 years after lease expires
Invitation to Tender	1 year from end of contract
Unsuccessful tender documents	1 year after date of decision
Successful tender document	3 years after completion of contract
Interview panel – report and notes of proceedings	1 year from end of contract
Reports from contractors	2 years from end of contract
Final accounts	6 years from end of contract
Minutes and papers of meetings	2 years from end of contract
Forms of variation	2 years from end of contract
Extensions to contract	2 years from end of contract

Health and Safety

Description	Disposal Period
Reporting of Injuries and Occurrences	3 years

Information Management Records

Description	Disposal Period
Information about the number of FOI requests answered and their outcomes, e.g., Enquiry Template	5 years
Policy records and internal documents on implementation and compliance with the FOI Act	1 year after policy/procedures have been superseded
Records relating to FOI requests including the information subject to the request	3 years after date of request

Record Retention and Disposal policy	When superseded

Employee Records

Description	Disposal Period
Contract of employment	2 years after resignation
Job History and actions	2 years after resignation
Assessment reports for last 5 years of service	2 years after resignation
Resignation letters	2 years after resignation
Health referrals including medical reports	2 years after resignation
Papers relating to any injuries on duty	2 years after resignation
Medical/Self Certificates	2 years after resignation

Membership, Press and Events Records

Description	Disposal Period
Press releases	7 years
Press cuttings	1 month
Operational notes (notices to press about forthcoming events or conferences)	3 months
Press conference reports/previews	3 years
Reports on media public relations	7 years
Image library	When no longer required
Event Correspondence and papers	3 years
Event reports	3 years
Events Brochures and guides	3 years
Events delegates lists	1 year after attendance at event
Evaluation reports	1 year after event
Membership records	3 years after ceasing to be a member

4. **Data Privacy Policy -** This framework sets out the organisation's approach to data security.

   Information security is the sixth data protection principle. In practice, it means AELP must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised.

   AELP designs and implements systems that are securely organised to fit the nature of the personal data held and to minimise harm that may result from a security breach. Policies and procedures are in place to secure data and apply to systems covering secure filing of documents and IT systems that are regularly backed up both on site and off site. In addition, AELP personnel receive training and apply a clear desk approach and password management.

   A privacy notice is published on AELP website, advising members and staff what the collected data is being used for, how long it is kept for and who it will be shared with.

   AELP collects personal data (e.g. name, address, email, fax and telephone number) through membership services; or by individuals who purchase a service or communicate or raise questions with AELP.

   Additional information about actual or prospective members from third party sources is also occasionally collected. Mostly this will be personal data such as a person's work email or telephone number, or details of their role within a business and this information is generally used in support of AELP research activities.

   AELP will only ever use personal data with consent:

   - for AELP's lawful interests such as internal record keeping and maintaining contact.
   - to enter into, or perform, a contract
   - to comply with a legal duty

   We only use personal information for the purpose it was collected. AELP will never sell personal data or share it with third parties who might use it for their own purposes.

4.1. Individuals' rights

AELP wants to ensure individuals remain in control of their personal data. Part of this is making sure individuals entering into business relations with AELP understand their legal rights, which (for individuals) are as follows:

- Confirmation about whether or not AELP has an individual's personal data and, if we do, the right to obtain a copy of it (this is known as a subject access request)
- The right to have inaccurate data rectified
- The right to object to personal data being used for marketing or profiling

There are exceptions to these rights and, although AELP will always try to provide a satisfactory response, there may be situations where we are unable to do so. If an individual is not happy with the response they receive, or they believe that their data protection or privacy rights have been infringed, they should contact the UK Information Commissioner's Office, which oversees data protection compliance in the UK. Details of how to do this can be found at www.ico.org.uk

Individuals have a right, commonly referred to as subject access, to request information about the details an organisation holds about them. AELP's SAR can be seen at appendix (i).

AELP will not release information about other people, unless they are acting on behalf of another person. Any such requests are treated with caution, and assurances are obtained about the validity of such requests.

Subject access requests should be made be in writing or by email to AELP. Verbal requests may be accepted at a Manager's discretion but should be discouraged. An individual who makes a request is entitled to be:

- told whether any personal data is processed
- given a description of the personal data, the reasons it is processed, and whether it will be given to any other organisations or people
- given a copy of the information comprising the data; and given details of the source of the data (where this is available)

AELP must respond to a subject access request without delay, and at the latest within one month. It is possible to extend the period of compliance by two months where requests are complex and numerous, but AELP must inform individuals within one month of submitting the request to provide an explanation for any delay. AELP's data handling procedure for staff is at Appendix (ii).

The legislation recognises that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Some types of personal data are exempt from the right of subject access e.g. taxation information, and so cannot be obtained by making a subject access request.

Repeated or multiple requests from individuals do not need to be actioned unless there has been a change in the data held since the previous request. The principle is based upon releasing only the information held at the time of the request.

4.2. Processing data

The GDPR mandates a Data Protection Impact Assessment (DPIA) is conducted where data processing "is likely to result in a high risk to the rights and freedoms of natural persons".

A DPIA is a process to help to identify and minimise the data protection risks of a project, and must be done for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

A DPIA must: describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks.

To assess the level of risk, both the likelihood and the severity of any impact on individuals must be considered. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. The DPO (if there is one) and, where appropriate, individuals and relevant experts should be consulted.

The ICO must be consulted if a high risk that cannot be mitigated is identified before starting processing. They will provide written advice within eight weeks, or 14 weeks in complex cases. In appropriate cases a formal warning may be issued not to process the data, or the ICO may ban the processing altogether.

DPIAs can also be used to support the accountability principle, helping organisations to comply with the requirements of the GDPR and demonstrate that appropriate measures have been taken to ensure compliance.

AELP will complete DPIAs to help to identify, assess and mitigate or minimise privacy risks with data processing activities, particularly when a new data processing process, system or technology is being

introduced. They will be conducted as early as possible within any new project lifecycle, so that its findings and recommendations can be incorporated into the design of the processing operation. The AELP DPIA is at Appendix (iii).

A DPIA will typically consist of the following key steps:

- Identify the need for a DPIA
- Describe the information flow
- Identify data protection and related risks
- Identify data protection solutions to reduce or eliminate the risks
- Sign off the outcomes of the DPIA
- Integrate data protection solutions into the project

Known as privacy by design, the embedding of data privacy features into the design of projects can have the following benefits:

- Potential problems are identified at an early stage
- Addressing problems early will often be simpler and less costly
- Increased awareness of privacy and data protection across the organisation
- Organisations will be less likely to breach the GDPR
- Actions are less likely to be privacy intrusive and have a negative impact on individuals

The GDPR does not specify which DPIA process must be followed, but instead allows for organisations to introduce a framework that complements their existing working practices. Conducting privacy impact assessments code of practice, from the Information Commissioner's Office (ICO), is an example of such a framework.

4.3. Potential Consequences of non-compliance under the GDPR

The ICO has the authority to mete out more substantial fines to organisations that don't comply with the new regulations. If found to be non-compliant, an organisation could face one of the GDPR's two-tiered fines: a fine of up to €10 million (roughly £8 million) or 2 per cent of annual turnover—whichever is higher—for NOT:

- Properly filing and organising personal data records
- Notifying the supervising authority (such as the ICO) and affected individuals about a breach
- Conducting the necessary preliminary impact assessments

A fine of up to €20 million (roughly £16 million) or 4 per cent of annual turnover—whichever is higher—can be given for violating:

- The basic principles related to data security
- Consumer consent

Even though an organisation could receive either fine, they are most likely to receive the more substantial fine for any violations in their digital marketing and advertisement practices.

4.4. Marketing under the GDPR

Privacy and Electronic Communications Regulations (PECR) have existed since 2003, and they are currently undergoing a major overhaul of updating electronic marketing rules to supplement GDPR. In GDPR's Marketing Guidelines, the main focus is about the protection of personal data, and specifically relates to electronic communications.

The proposed revisions to PECR include simplifying cookies, banning unsolicited electronic communications if users haven't given their consent and incorporating the GDPR's two-tiered fine structure. PECR's biggest proposed change is making all forms of electronic marketing reliant upon opt-in consent.

This is similar to the GDPR and means that pre-ticked boxes will no longer be acceptable, even with business-to-business communications. Under the GDPR, organisations must identify and provide a lawful basis to process personal data, which is any information that can be used to identify an individual. For example, joe.public@anybusiness.com would classify as personal data that requires Joe's consent before you can market to him through email, even though it's a business address.

EU lawmakers intended for these proposed changes to PECR to take effect on the same day as the GDPR, although there is significant doubt as to whether they will make that deadline. Regardless, as PECR sits alongside the GDPR, organisations should follow the revised marketing guidelines to avoid potential fines.

4.5. Consent

The GDPR has adjusted the guidelines on how organisations can manage their digital marketing and advertising efforts. Obtaining consent is now central to establishing the necessary lines of communication with individuals. Making that connection is not always easy, and failure to obtain proper consent puts the organisation at risk of significant fines. However, by highlighting the quality and benefits of what is done to manage and protect an individual's data, is more likely to result in their consent.

AELP will only use personal information (such as email addresses) to market and promote our services to other businesses if consent has been obtained. In order for AELP to remain compliant with the GDPR in electronic marketing and advertising efforts, the process for obtaining consent must meet the following standards:

- Requests for consent must be separate from other terms and conditions, and should not be a precondition of signing up for a service.
- Active opt-in—AELP cannot use pre-ticked opt-in boxes.
- Individuals must be given options to consent to different types of processing
- AELP and any third parties that will be relying on the individuals' consent must be named.
- Documented—records kept to demonstrate what the individuals have consented to, what they were told, and when and how they consented.
- Individuals must be informed that they have the right to withdraw their consent at any time and provided with an explanation of how they can do that.

4.6. Working with Third Parties

AELP will not disclose personal data to third parties, unless there is a legal requirement to do so. However, as more information that affects a business is created and stored elsewhere, it is essential to establish how the organisation operates and shares information with stakeholders, partners and suppliers.

AELP cannot control how 3rd parties manage personal data, but recognises that all organisations are bound by GDPR regulations, and failure to adhere to regulations would result in considerable financial penalties for non-compliant bodies. Suppliers working with AELP will be expected to sign an agreement that includes GDPR compliance.

Consent by the individual underpins how AELP shares personal data with 3rd parties. For requests from 3rd parties to obtain personal data, AELP will only do so once consent has been given by the individual concerned, unless there is a legal requirement to disclose. Where there is a legal requirement to disclose personal data, e.g. to HMRC, access is restricted only to those authorised to use the data, which is password protected.

The AELP website may contain links to other websites. We do not control those other sites and we cannot be responsible for the content of those sites or for the protection of any information individuals provide to other sites (which are not governed by this privacy policy).

We accept no responsibility or liability for other websites, and individuals should therefore exercise caution when entering personal information online and look at the privacy statement applicable to the website in question.

5. Data Breach and Incident Management Policy

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach if any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

When a personal data breach has occurred, individuals will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, the ICO must be informed and if it's unlikely it will not need to be reported. However, if it is not reported, the reasons why should be clearly justified and documented.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

> *"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."*

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. All will need to be assessed on a case by case basis, looking at all relevant factors to facilitate decision-making about whether or not the relevant supervisory authority and the affected individuals are notified.

Recital 87 of the GDPR makes clear that when a security incident takes place, organisations should

establish whether a personal data breach has occurred immediately, and if so, to report it to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.

AELP will assess any breach of data for whether it is likely to result in a high risk of adversely affecting individuals' rights and freedoms: if so individuals must be informed without undue delay. An assessment will also be made about breach detection, investigation and internal reporting procedures to assess if they have been observed in an appropriate and timely way including:

- recognising a personal data breach
- understanding that a personal data breach isn't only about loss or theft of personal data
- preparing a response plan for addressing any personal data breaches that occur
- allocating responsibility for managing breaches to a dedicated person or team
- escalating a security incident to the appropriate person or team within AELP to determine whether a breach has occurred

All AELP staff must report data protection breaches as soon as they become aware of them. This will allow the appropriate personnel to investigate further and take the appropriate steps to fix the issue in a timely manner. The policy can be actioned by the following steps:

- Reporting information losses
- Reporting information security breaches
- Incident management and escalation
- Back up and disaster recovery
- Business continuity management

Staff training explains the importance of processing personal data lawfully, and the potentially serious consequences of failing to comply with GDPR. It is a central element of AELP policy, and provides detailed explanation of the processes for handling data; managing data breaches; and the roles and responsibilities of all staff.

The AELP Risk Register includes data breaches and has clear mitigating actions and a Data Inventory spreadsheet will be used as the reporting and control document. A copy of the Data Inventory is at Appendix (iv).

Annex A

Questions and Answers

What is a personal data breach?

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- IT equipment and mobile devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

What breaches should the ICO be notified of?

Examples of personal data breaches include:

- Theft of a customer database
- An IT services firm (the processor) detects an attack on its network that results in personal data about its clients being unlawfully accessed.
- A Contractor used to archive and store data containing personal information reports there has been unauthorised access and data has possibly been stolen.

What information must a breach notification to the supervisory authority contain?

When reporting a breach, the GDPR says the following should be provided:

- a description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals and personal data records concerned
- the name and contact details of the data protection officer (if there is one) or other contact point where more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

What if all the required information isn't available yet?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 34(4) allows organisations to provide the required information in phases, as long as this is done without undue further delay.

When do individuals need to be told about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says those concerned must be informed directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is greater than notifying the ICO. An assessment will be required of both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, those affected must be informed immediately, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

A "low risk" breach e.g. information released to a Trusted Body such as HMRC, will need to be reported to the individual.

What happens if we fail to notify?

Failure to notify a breach when required to do so can result in a significant fine of up to 10 million euros or 2 per cent of an organisation's global turnover. The fine can be combined with the ICO's other corrective powers under Article 58. It is important therefore to ensure there is a robust breach-reporting process in place.