

# General Data Protection Regulations (GDPR) Retention Policy



## Policy Statement

EOS Europe Ltd (EOS Europe) recognises that managing personal data and information is integral to its regulatory compliance function. EOS Europe views these as one of its primary responsibilities and as the key to good business practice,

EOS Europe needs to collect and process personal data about the people it deals with in order to carry out its business and provide its services.

Such people include, but are not limited to, employees (present, past, and prospective), contractors, customers, suppliers, and other business contacts. The data may include identifiers such as name, address, email address, date of birth, National Insurance Numbers, etcetera. It may also include private and confidential information and special categories of personal data.

In addition, EOS Europe may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded, and used (e.g. on a computer or other digital media, on hardcopy, paper, or images, including CCTV), this personal information must be dealt with properly to ensure compliance with data protection legislation:

- the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) implement the GDPR in the UK.

The lawful and proper treatment of personal information by EOS Europe is essential to the success of our business and to maintaining the confidence of our employees, customers, and its supply chain. EOS Europe must ensure that it processes personal information lawfully and correctly.

EOS Europe has aligned its procedures and processes with the definition of 'personal data' provided in DPA2018 to comply with the Act.

To assist individuals with duties under the DPA2018, EOS Europe has created a set of guidelines (attached to this Policy) for the management and security of personnel data and information that it holds within the meaning of the law.

This policy will be monitored periodically to ensure that the objectives are achieved and will be reviewed and revised where legislative or Company changes are deemed necessary.

A handwritten signature in black ink, appearing to read 'G McLeod'.

George McLeod,  
Managing Director  
25<sup>th</sup> March 2025

Policy No	Rev	Iss	Title	Page No:
EOS-p-255	1	1	General Data Protection Regulations (GDPR) Policy	1

# General Data Protection Regulations (GDPR) Retention Policy



## EOS Europe Employment records: Retention and Erasure guidelines

### About these guidelines:

These guidelines support EOS Europe's data privacy policy and are intended to ensure that EOS Europe processes personal data in accordance with personal data protection principles, in particular, that:

- Personal data must be collected only for specified, explicit, legitimate purposes. It must not be further processed in any manner incompatible with those purposes.
- Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. When personal data is no longer needed for specified purposes, it is deleted or anonymised as provided by these guidelines.
- Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
- Personal Data must not be kept in identifiable form for longer than necessary for the purposes for which it is processed.
- Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

The Data Protection Officer (DPO) is responsible for overseeing these guidelines. Any questions about the operation of the guidelines should be submitted to the DPO.

### Definition:

The GDPR definition of "personal data" covers any information relating to an identified or identifiable natural person—i.e., living individuals. Pseudonymised personal data is covered; however, anonymised or aggregated data is not regulated by the GDPR or DPA2018, provided the anonymisation or aggregation has not been done in a reversible way. Individuals can be identified by various means, including their name and address, telephone number or Email address, Number, and NI Number.

The GDPR defines special categories of personal data (previously referred to as sensitive personal information) as information related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data • Biometric data
- Health data
- Sexual history and sexual orientation
- Criminal data

### Location of Employment Records

EOS Europe holds employment records and can be contacted with any enquiries about the individual's data.

Policy No	Rev	Iss	Title	Page No:
EOS-p-255	1	1	General Data Protection Regulations (GDPR) Policy	2

# General Data Protection Regulations (GDPR) Retention Policy



## Keeping Information Up to Date

EOS Europe needs to ensure that personal details are up-to-date and accurate. When individuals first start working for EOS Europe, the company records their name, address, next of kin, and contact details.

If any of these changes occur, the individual should inform the company immediately. The individual is invited to review and update personal information on a regular basis.

These provisions complement the data subject rights in the data privacy notice.

## General Principles on Retention and Erasure

EOS Europe's approach to retaining data and personal information is to ensure that it complies with the data protection principles referred to in these guidelines and, in particular, to ensure that:

- Employment records are regularly reviewed to ensure they remain adequate, relevant, and limited to what is necessary to facilitate the individual's work for EOS Europe.
- Employment records are kept secure and protected against unauthorised or unlawful processing and accidental loss, destruction, or damage.
- Where appropriate, EOS Europe causes anonymisation to prevent the identification of individuals.
- When records are destroyed, whether held as paper or electronic, EOS Europe will ensure they are safely and permanently erased.

## Retention and Erasure of Recruitment Documents

EOS Europe retains personal information following recruitment exercises to demonstrate if required, that candidates have not been discriminated against on prohibited grounds and that recruitment exercises are conducted fairly and transparently.

EOS Europe's candidate privacy notice advises candidates how long EOS Europe expects to keep their personal information once a recruitment decision has been communicated to them.

This is likely to be for six months from the communication of the recruitment exercise's outcome, which considers both the time limit to bring claims and the time limit for claims to be received. EOS Europe information relating to successful candidates will be transferred to their employment records with EOS Europe.

This will be limited to the information necessary for the working relationship and, where applicable, that is required by law.

The Office Manager will hold information, in both paper and electronic form, following a recruitment exercise. That information will be destroyed in accordance with these guidelines.

Policy No	Rev	Iss	Title	Page No:
EOS-p-255	1	1	General Data Protection Regulations (GDPR) Policy	3

# General Data Protection Regulations (GDPR) Retention Policy



## Retention and Erasure of Employment Records

EOS Europe follows the recommended retention periods for employment records as the law prescribes. The table below outlines these periods. However, we also consider legal risk and may retain records for up to seven years or more after the end of your employment or work with us.

Type of Employment Record	Retention Period
<b>Recruitment</b>	
Recruitment records These may include: <ul style="list-style-type: none"> <li>Completed online application forms or CVs.</li> <li>Assessment exercises or tests.</li> <li>Notes from interviews and short-listing exercises</li> <li>Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.)</li> <li>Criminal records checks. (These may be transferred to a successful candidate's employment file if relevant to the ongoing relationship.)</li> </ul>	Six months after notifying candidates of the outcome of the recruitment exercise.
<b>Immigration checks</b>	Three years after the termination of employment
<b>Contracts</b>	
These may include: <ul style="list-style-type: none"> <li>Written particulars of employment.</li> <li>Contracts of employment or other contracts.</li> <li>Documented changes to terms and conditions.</li> </ul>	While employment continues for seven years after the contract ends.
<b>Collective agreements</b>	
Collective workforce agreements and past agreements that could affect present employees	A copy of a relevant collective agreement retained on an employee's record will remain for seven years after employment ends.
<b>Payroll and wage records</b>	
Details on: <ul style="list-style-type: none"> <li>Overtime.</li> <li>Bonuses.</li> <li>Expenses.</li> <li>Benefits in kind.</li> </ul>	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to incidents that cause injury, they should be retained for seven years after employment ends.
Current bank details	After the end of employment, bank details will be deleted as soon as possible once final payments have been made.
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to incidents that cause injury, they may be retained for seven years after employment ends.
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which

Policy No	Rev	Iss	Title	Page No:
EOS-p-255	1	1	General Data Protection Regulations (GDPR) Policy	4

# General Data Protection Regulations (GDPR) Retention Policy



	payments were made. However, given their potential relevance to Incidents that cause injury, they may be retained for seven years after employment ends.
Records about hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to Incidents that cause injury, they may be retained for seven years after the working relationship ends.
Record of advances for and loans to employees	While employment continues for seven years after employment ends,
<b>Personnel records</b>	
These include: <ul style="list-style-type: none"> <li>• Qualifications/references.</li> <li>• Consents for the processing of special categories of personal data.</li> <li>• Annual leave records.</li> <li>• Annual assessment reports.</li> <li>• Disciplinary procedures.</li> <li>• Grievance procedures.</li> <li>• Death benefit nomination and revocation forms.</li> <li>• Resignation, termination, and retirement.</li> </ul>	While employment continues for three years after employment ends.
<b>Records in connection with working time</b>	
Working time opt-out	Three years from the date on which they were entered into.
Records to show compliance, including: Timesheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.
<b>Maternity records</b>	
These include: <ul style="list-style-type: none"> <li>• Maternity payments.</li> <li>• Dates of maternity leave.</li> <li>• Period without maternity payment.</li> <li>• Maternity certificates showing the expected week of confinement.</li> </ul>	Four years after the end of the tax year, the maternity pay period ends.
<b>Incident records</b>	
These are created for any reported incident, death, or injury in connection with work and are included for insurance purposes.	For at least four years from the date the report was made.

Policy No	Rev	Iss	Title	Page No:
EOS-p-255	1	1	General Data Protection Regulations (GDPR) Policy	5