Contract Services Europe

Records Retention Policy

1. POLICY STATEMENT

This Policy sets out the obligations of **DPS Contract Services** (hereinafter referred to as the "**Company**") regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The Company only ever retains records and information for legitimate or legal business reasons and always complies fully with EU data protection laws, guidance and best practice.

2. PURPOSE

This Policy sets out the type(s) of personal data held by the Company, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy (link).

3. OBJECTIVES

The GDPR impose obligations on the Company, as a Data Controller, to process personal data in a fair manner which notifies data subjects of the purposes of data processing and to retain the data for no longer than is necessary to achieve those purposes.

The Company's objectives and principles in relation to Data Retention are to:

- Set out limits for the retention of personal data and ensure they are complied with
- Ensure the Company complies fully with its obligation and rights of data subjects under the GDPR
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each bodies rules or terms.
- Mitigate against risks or breaches in relation to confidential information

4. SCOPE

This policy applies to all persons within the Company (meaning permanent, fixed term, temporary staff and sub-contractors engaged with the Company). Adherence to this policy is mandatory and non-compliance could lead to disciplinary or contractual action.

5. RESPONSIBILITIES

Heads of departments and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure

that the records created, received and controlled within the purview of their department, and the systems (electronic or otherwise) and procedures they adopt, are managed in a way which meets the aims of this policy.

Where a DPO has been designated, they must be involved in any data retention processes and records or all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with the Company's protocols.

6. GENERAL DATA PROTECTION REGULATION (GDPR)

The Company needs to collect personal information about job applicants, the people we employ, work with or have a business relationship with to effectively and compliantly carry out our everyday business functions and activities, and to provide the services defined by our business type. This information can include but is not limited to, name, address, email address, date of birth, identification number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation, EU data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

7. GUIDELINES & PROCEDURES

The Company retains data records efficiently and systematically, in a manner consistent with the GDPR requirements, ISO 9001:2015 and regulatory Codes of Practice on Records Management. This policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be retained to provide information about, and evidence of the Company's transactions, customers, employment and activities. Retention schedules will govern the period that records will be retained and can be found in the **Record Retention Periods** table at the end of this document.

7.1 Retention Period Protocols

All company and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within the Company, we:

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained
- Establish and verify retention periods for the data, with special consideration given in the below areas:
    - the requirements of the Company
    - the type of personal data

- the purpose of processing
- lawful basis for processing
- the categories of data subjects

- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, the Company will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices (link to privacy notice)
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered

7.2 Information Asset Owners

All systems and the records they contain have Information Asset Owners (IAO) throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, business area and level of access to the data required. The IAO is recorded on the Retention Register and is fully accessible to all employees. Data and records are never reviewed, removed, accessed or destroyed without the prior authorisation and knowledge of the Information Asset Owner.

7.3 Suspension of Record Disposal for Litigation or Claims

If the Company is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our Company, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

7.4 Storage & Access of Records and Data

Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are reviewed, archived or confidentially destroyed dependant on their purpose.

7.5 Expiration of Retention Period

Once a record or data has reached its designated retention period date, the IAO should refer to the retention register for the action to be taken.

7.6 Destruction and Disposal Of Records & Data

All information of a confidential or sensitive nature on paper or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

The Company is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

7.6.1 Paper Records

Due to the nature of our business, the Company retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. The Company utilises a Professional Shredding Service Provider to dispose of all paper materials.

Employee shredding machines and confidential waste disposal units are made available throughout the building and where we use service provider disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

7.6.2 Electronic & IT Records and Systems

The Company uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed.

Only the IT Department can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally. IT equipment follows a fully auditable disposal process involving a combination of secure electronic and physical destruction methods to permanently erase data records prior to disposal of the asset.

In all disposal instances, the IT Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Department is responsible for liaising with the information Asset Owner and updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and IT Department to ensure that all relevant data has been sufficiently removed from the IT device before requesting disposal.

7.6.3 Internal Correspondence and General Memoranda

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support (i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed).

Where correspondence or memoranda that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases.

8. ERASURE

In specific circumstances, data subjects' have the right to request that their personal data is erased, however the Company recognise that this is not an absolute 'right to be forgotten'. Data

subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation

For further information on other aspects of data erasure process and compliance, please refer to the Company's Procedure for Handling of Individual Rights (link)

8.1 Special Category Data

In accordance with GDPR requirements, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

9. COMPLIANCE AND MONITORING

The Company are committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners (?) are tasked with ensuring the continued compliance and review of records and data within their remit.

10. RETENTION PERIODS

As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

11. RETENTION REGISTER

Recruitment Data

DATA TYPE	RETENTION PERIOD	Why is it collected	Who can access	ASSET OFFICER	SECURITY	GDPR REASON	FINAL DISPOSITION
Information, data or record	**Period for retaining record & accompanying notes**			**Who is responsible for reviewing periods**	**Destroy, archive, review etc**		
Application form	2 years	To establish suitability for post	Contract Services(CS) Team Interviewing Manager		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Consent	Confidential shredding OR Safe/secure deletion Retain an anonymised sample for archival purposes
CV	2 years after date employment ceases. Unsuccessful candidates CVs 2 year	To establish suitability for post To inform of job opportunities	CS Team Interviewing Manager		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Consent	Confidential shredding OR Safe/secure deletion Retain an anonymised sample for archival purposes
Pre-Employment Medical	2 years after date employment ceases.	To establish if they are medically fit for position to	CS Team Interviewing Manager		Stored in lockable filing cabinet – CS own access to files	Consent	Confidential shredding OR Safe/secure deletion

		which they have applied			If stored as e-copy; access will be password protected		
Interview questions and interview notes	2 years	To record questions asked and responses to ensure compliance with Equality act and to establish suitability for post	CS Team Interviewing Manager		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Consent	Confidential shredding OR Safe/secure deletion
Offer letters	2 years after leaving date	To record contractually what was offered / committed to the candidate	CS Team Interviewing Manager		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Consent	Confidential shredding OR Safe/secure deletion
Recruitment consent form	2 years after leaving date	To establish consent to process data / store data	CS Team Data Controller		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected		Confidential shredding OR Safe/secure deletion

Payroll information							
Payroll records	7 years after leaving	To enable pay to be processed and payments to be made	Finance Dept CS Dept		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
Personnel Files							
Copy of passport (or other right to work documents)	2 years after date employment ceases	To establish if they have the right to work in the EU.	CS Team		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
Redundancy details, calculations of payments & refunds	7 years from the date of redundancy	To enable processing and recording of redundancy.	CS Team Finance Dept		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion

Sick certificates & self-certificates	6 years	To enable processing and recording of sick leave	CS Team		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
References	6 years after start date	To establish that they are suitable for the job.	CS Team Hiring Manager		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Consent	Confidential shredding OR Safe/secure deletion
Contract of employment	6 years after leaving date	To record their contractual terms of employment	CS Team Hiring Manager		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
Confidentiality Letters	For the duration of the confidentiality covenant after leaving and 6 months thereafter (in case there is a later found breach)	To record any data confidentiality contractual terms	CS Team Hiring Manager		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion

Name & Address	2 years after leaving	To uniquely identify and employee	CS Team		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
PPS Number	2 years after leaving	To uniquely identify the employee for government communicatio n purposes	CS Team Finance Dept		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
DOB	2 years after leaving	To know their age for pension and retirement related purposes	CS Team Finance Dept		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
Details of next of kin	Upon leaving	To make contact in emergencies	CS Team		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Consent	Confidential shredding OR Safe/secure deletion

Qualification certificates	2 years after leaving	To record competencies and qualification obtained	CS Team		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Consent	Confidential shredding OR Safe/secure deletion
Performance scoring / rating documents	2 years after leaving	To record any performance rating data that may influence pay decisions	CS Team		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Consent	Confidential shredding OR Safe/secure deletion
Disciplinary warnings and investigations	9 months after expiry of warning 12 months after completion of investigation	To record any disciplinary warnings issued To make a record of any investigations that have been carried out.	Line Manager Investigation Officer		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
Grievances	12 months after completion of investigation	To make a record of any grievances or grievance investigations	Line Manager Grievance Manager		Stored in lockable filing cabinet – CS own access to files	Legal	Confidential shredding OR Safe/secure deletion

		that have been carried out and a record of any agreed outcomes			If stored as e-copy; access will be password protected		
Absence data	12 months after leaving	To record number of days absence policy monitoring			Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
Client Data							
Client Correspondence details – name, address, telephone number, email address	If linked to a vendor, then held indefinitely until asked to be removed by vendor	To allow correspondence between DPS Contract Service and Clients	CS Team		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion
Client Contract Data – This may include name, BIC, IBAN, Account Number, Account name	If linked to a vendor, then held indefinitely until asked to be removed by vendor. Financial data to be held for seven years	To enable financial transactions between DPS Contract Service and Clients	CS Team Finance Department		Stored in lockable filing cabinet – CS own access to files If stored as e-copy; access will be password protected	Legal	Confidential shredding OR Safe/secure deletion