|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Name**  | **Document No.** | **Issue No.** | **Effective Date** | **Review Date** |
| GDPR Personal Data Retention Period | 1 | 2 | November 2020 | November 2021 |

**Approvals**

The signatures below certify that this procedure has been reviewed and accepted, and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Name** | **Signature** | **Position** | **Date** |
| **Prepared by** | Grace Kelly |  | GDPR Administrator | November 2020 |
| **Reviewed by** |  |  |  |  |
| **Approved by** |  |  |  |  |

**Amendment Record**

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Issue No.** |
| November 2020 | Update review to ensure ongoing compliance | 2 |
|  |  |  |

**1. Introduction & Purpose**

Regulations protecting personal data state that they are collected for a limited period of time and must be destroyed once this time is up.

This requires defining retention periods right from the time when the processing system is designed and ensuring that they are complied with.

Under the GDPR and Data Protection Acts 1988-2018, DPD Ireland, as a *Data Controller*, has a legal responsibility to:

* Obtain and process personal data lawfully, fairly and in a transparent manner;
* Keep it only for one or more specified and explicit lawful purpose(s);
* Process it only in ways compatible with the purpose of which it was given initially;
* Keep data accurate, relevant and not excessive;
* Retain it no longer than is necessary for the specified purpose or purposes;
* Keep personal data safe and secure.

**2. References**

| **Standard** | **Title & Description** | **Clause** |
| --- | --- | --- |
| Article 13 GDPR | Information to be provided where personal data are collected from the data subject |  |
| Data Protection Acts 1988-2018 | To give further effect to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); to give effect to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA; to give further effect to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January 1981 and for those and other purposes to amend the Data Protection Act 1988; to provide for the consequential amendment of certain other enactments; and to provide for related matters. |  |
|  |  |  |

**3. Terms & Definitions**

| **Term** | **Definition** |
| --- | --- |
| D.P.O | Data Protection Officer |
| Active Database | Data that is regularly used by the departments/divisions/business units tasked with data processing (e.g. data on a customer that is used to complete a contract) |
| Intermediate archives | Data that is no longer used primarily for processing but which still has an administrative usefulness, e.g. should a dispute arise or to meet a legal or regulatory requirement. Any data archived in this way should be deleted once the reason for retaining the data no longer applies.For example, data that is archived to prove a legal right must be deleted once the statute of limitations for this legal action is reached. |
| Definitive Archives | Data retained solely for archive purposes in the public interest, for scientific or historic research purposes or for statistical purposes, so long as suitable technical and organisational measures are in place. If these reasons are not present, the data must be destroyed at the end of the intermediate archival period. Otherwise, irreversible anonymisation can allow retaining data after their initial processing period has expired. |
|  |  |
|  |  |
|  |  |

## 4. Application & Scope

The general principle is that personal data is retained for **a period that does not exceed the period required to achieve the purpose** that the data was collected for (Art 5. GDPR) and our general obligations under GDPR and the Data Protection Acts 1988-2018.

Every operational data processing department manager should therefore, when designing the processing, determine a data retention duration that is consistent and justified in view of the processing goals set out.

The manager may also take account of the need to retain certain kinds of data for a legally mandated period of time in case of dispute, so that proof can be provided.

Lastly, there may be legal requirements to retain data to fulfil accounting, tax or social welfare requirements.

**5. Responsibilities**

All department managers are responsible for reviewing the personal data

stored and the required retention periods. The DPO along with department managers are

responsible for checking that the retention durations observed match the declared durations..

**6. Process**

**6.1 Persons whose data is collected are informed of the duration that this data will be retained for**

The duration that your personal data is retained for is part of the mandatory information that must be provided.

When the retention duration cannot be specified, the statement will set out the criteria used to determine it (Art. 13 GDPR) and the Data Protection Acts 1988-2018.

**6.2 The retention duration is declared in the Processing Register kept by the DPO**

The duration is part of the data that must be recorded in the Processing Register.

Further, always ensure that the declared retention durations are actually applied

**6.3 Once the data retention duration is reached, the data must be deleted.**

Data that is no longer of any use will be deleted as soon as the planned retention duration expires.

Data that is covered by a legally mandated period of time in case of dispute, so that proof can be provided as well as that covered by legal requirements to retain data to fulfil accounting, tax or social welfare requirements, etc., are moved to, or stored in an intermediate archival system subject to restricted and controlled access. After the corresponding durations (statute of limitations, dispute related or those determined by the law), the data will be deleted.

In the end, after the retention period expires, the person in charge of processing needs to proceed to destroy or eliminate all of the data when retained on paper or delete it when on electronic media.

Data cannot be used for other purposes, except where applicable for historical, statistical or scientific purposes.

Where the law calls for a requirement to archive data or where the person in charge of processing wishes to retain data to retain proof should any dispute arise, be sure to only archive data that is useful for complying with the necessary obligation, or to prove legal rights. The person in charge of processing must therefore selectively sort from all of the data collected to retain only data that is essential.

It is preferable that the deletion of this data be performed automatically. Where this is not possible, deletion may be handled by a procedure. The person in charge of processing will ensure that this data is actually deleted.

**6.4 Access Rights by the Persons Concerned**

Any person who exercised their access tight must be able to see all of the data relating to them, whether stores in an active database or archived.

**6.5 Failure to Comply with these Rules Exposes the People in charge of Processing to Penalties**

Failure to set a retention duration or failure to comply with the durations that are set may trigger an administrative fine that can reach 4% of the groups annual worldwide sales.

##  7. Archiving Personal Data

**7.1 The Archival Mode is Determined Freely (See Fig1.1)**

The choice of archival mode is left up to the person in charge of processing. Data can be archived:

* In a specific archive database that is separate from the active database, with access restricted solely to people with a need to know relating to their position (e.g. the legal department), or
* In the active database so long as the archived data is isolated by a logical separation (through managing access rights and permissions) to make them inaccessible to people who no longer have any interest in processing them
* For definitive archives (i.e. only data of a historical, scientific or statistical interest), it is recommended retaining them on a separate media that is not accessible by production systems, permitting only separate, one-off and clearly motivated access to a specific department that alone is permitted to access them (e.g. the archives department where one exists).

**7.2 Archive Storage must be Secure**

Technical and organisational measures need to be taken to protect archived data (from deletion, loss, alteration, release or unauthorised access, etc.). These measures need to ensure a degree of security that is in line with the risks and type of data involved, in line with in-house rules set out by the CIO. Just as IT security measures are essential physical security measures too are essential, especially when files are archived on paper.

When archive storage is entrusted to a subcontractor, the person in charge of processing will ensure that their contractor offers sufficient guarantees in security and confidentiality terms for the data entrusted to them.

|  |
| --- |
| **Data Retention Period – HR Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Payroll and Tax records | Contains personal data, bank account details, PPS Number | Revenue Commissioners - All employee payroll and tax records be retained for 7 years from the end of the financial year following termination of employment, or to the end of any enquiry by the Revenue Commissioners. |
| Payslips and records relating to wages | This may include contact details, date of birth, curriculum vitae, work and educational history, referee name, interview notes, related documentation etc | The National Minimum Wage Act 2000 (Section 22) - Payslips must be retained for at least 3 years from the date of their making to show compliance with the Act’s provisions, for example, payslips showing the employees were paid at least minimum wage. |
| Recruitment related data |  | Employment Equality Acts 1998 – 2015 - There is no statutory retention period for personal data relating to unsuccessful job candidates. Individuals have a maximum of 12 months to refer a complaint to the Workplace Relations Commission under the Employment Equality Acts 1998 – 2015. It is recommended therefore that such records are retained for at least 12 months from the date the position is filled to be able to defend any claim to the WRC. The Data Protection Commission considers a retention period of 1 full year to be appropriate in situations like this. |
| Terms and Conditions of employment | This may include personal data contained in contracts of employment and all related documentation | The Terms of Employment (Information) Act 1994 – 2012 - provides that an employee’s terms and conditions of employment must be retained for the duration of the employment and 1 year thereafter. The Statute of Limitations provides that a claim for breach of contract may be brought for up to 6 years from the date of breach. Plaintiffs have 1 year from the commencement of proceedings to serve such proceedings on a defendant. It is recommended, therefore, that all contractual and related documentation be retained for the duration of employment and 7 years from the termination or expiration of the contract. |
| Records relating to employees under 18 years. |  | Statutory retention period: 3 years. The Protection of Young Persons (Employment) Act, 1996, at section 15, provides for a 3 year retention period of employment records relating to persons under 18 years of age.  |
| Working time records | This will include details regarding weekly working hours, Annual leave and public holidays, rest breaks, PPS Numbers, statement of duties, name/address of each employee, copy of employee contracts, copy of any notices given to employees about starting and finishing times and notice of additional working hours | The Organisation of Working Time Act 1997 and related Regulations (The Organisation of Working Time Act, 1997, Section 25, and the Organisation of Working Time (Records) Prescribed Form and Exemptions, Regulations 2001) provide that working time records must be retained for a minimum of 3 years from the date of creation. |
| Records relating to collective redundancies | The Protection of Employment Acts, 1977-2007, at section 18, provides that where an employer has collective redundancies, it must retain the records to show that the provisions of the Act were complied with for a 3 year period | Statutory retention period: 3 years |
| Records relating to parental leave and Force Majeure Leave records. | Parental Leave Acts, section 27 | Statutory retention period: 8 years |
| Records relating to workplace accidents |  | 10 years from the date of an accident under Safety, Health and Welfare at Work (General Applications) Regulation 1993, section 60).  |
| Employment Permit Records  |  | 5 years or duration of employment |
| Carer’s Leave records |  | 8 years |

|  |
| --- |
| **Data Retention Period – Customer Services Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Financial data and credit card information  |  | For as long as it is necessary to process the transaction, including any queries which may arise. |
| Customer details obtained while interacting with DPD Ireland social media platforms  | To assist in completing orders, dealing with queries and complaints. | For as long as it is necessary to process the queries, complaints etc, including follow up queries, and not longer than one calendar month, or for longer to fulfil any legal requirements in the event of a dispute. |

|  |
| --- |
| **Data Retention Period – Pick-Up Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Contact information of customer - Personal details such as name, address, phone number and Eircode if given | Part of delivery process. As long as they remain a customer. A customer relationship is generally considered terminated from a data protection viewpoint if a transaction has not occurred within the previous year. The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | 12 months |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Gazzing Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Contact information of customer - Personal details such as name, address, phone number and Eircode if given etc. | As part of delivery of customer service requirements. The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | 6 months |
|  |  |  |

|  |
| --- |
| **Data Retention Period – IT Development/Support Departments** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| CCTV | Individuals have the right to access their personal data including their image in CCTV recordings. Requests shall be made in writing to the CCTV administrator, either by email or using a the DPD GDPR Data Access Form.  | One month unless copy requested within this time. |
| Copy of CCTV recording | Disclosure of images from the CCTV system is controlled and consistent with the purposes for which the system exists. All requests to access CCTV footage are channelled through the relevant CCTV administrator. All access to images is logged. Access requests by An Garda Síochána shall be processed where such processing is necessary and proportionate for preventing, detecting, investigating or prosecuting criminal offences. | Delete once purpose for which it was retained has been met and there is no longer a requirement to retain same. |
| Data in relation to computer hardware, software, systems, networks, printers and scanners etc | For the proper functioning of the company | 12 months |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Marketing Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Electronic marketing data – non-customers | The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | 12 months - Last point of contact provided target individual originally consented to receiving marketing data. |
| Electronic marketing data – customers  | The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | 12 months - From last point of contact with customer |
| Data collected may include customer data such as geographic location, gender, age, buying behaviours, and communication preferences. Information about Web site visitors, traffic, and other customer engagement activities could be included.  | The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | 12 months |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Quality Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| GDP – company information, terms of storage, contracts, details of all customer critical and non-critical incidents etc | For the effective and smooth operation of the business. The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | Two years |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Finance Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Financial data and credit card information | The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | For as long as it is necessary to process the transaction, including any queries which may arise. |
| Accounts, invoices, returns, audits, revenue, corporate governance, accounts payable, accounts received, banking details and other financial details |  | 6 years |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Network Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Finance and Regulatory |  | 6 years |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – HUB Operations** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Night sort, company details of external transport companies. |  | 6 years |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Health & Safety Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Health and Safety breaches, and details of same, data in relation to workplace accidents, first aid duties, health records and witness statements etc | To comply with regulations and existing legislation | 10 years |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Business Intelligent Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Processing of data in relation to business analytics, data mining, data visualization, data tools and infrastructure in relation to personal data. |  | **6 years** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – CRM Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Processing data in relation to interactions with customers and potential customers, storage of customer names, email addresses, company information, role and phone numbers etc | The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | 12 months |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Sales Department** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Sales teams capture and maintain and process information about who is buying the product, where buyers are located, buying patterns, and behaviours. Sales may also maintain and process information about customer references, success stories, and how prospective customers are progressing toward becoming new clients. Customer demographic and profile data linked to in-store and online purchasing history, Web site search terms, page views, social media posts, and other data may be gathered. | To assist the company in the pursuit of legitimate interests in sales growth and customer service. The legal basis for this processing is our legitimate interests, namely the proper management of our customer relationships. | 12 months |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Data Retention Period – Transport and Engineering Departments** |
| **Category of Personal Data** | **Reason for Processing** | **Maximum Retention Duration** |
| Data is relation to external transport details, design, construction, maintenance, and operation of transportation facilities. Logistics and associated data processed also includes purchasing and supplier management, materials management and manufacturing, inventory management and warehousing, distribution and transport, and customer service. Data in relation to organising schedules & routes, ensuring that vehicles are safe and meet legal requirements is also processed. | For the smooth and effective operation of the business | **6 years** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Appendix 1:** Fig 1.1

DELETE OR PURGE

DELETE OR PURGE DATA NOT COVERED BY A REQUIREMENT FOR INTERMEDIATE ARCHIVE STORAGE

**End of administrative use and start of final use**

**Collection**

**End of regular use**

**Data that is in regular use**

HR PD: Employment contract duration

Customer PD: Contract duration

Active database: As soon as the data is collected, it is regularly used for the declared purpose.

**Consequently: Data collection and storage will be accessible to everyone with a right to know.**

**Data that is of historical, scientific or statistical interest**

HR PD: After anonymisation (age, sex, staffer or civil servant, etc.)

Customer PD: After anonymisation (to be discussed but needs to reconcile the principle of the initial purpose of the processing.)

Definitive archive: Select data or information of permanent historical, scientific, statistical or public interest for understanding the business, the organisation involved, the population involved, etc.

**Comply with the initial purpose principle, if not, do not retain archives beyond the intermediate archive stage**

**Data that is still of administrative interest**

HR limitations) or a required retention duration (5 years from when the person leaves the company).

Customer PD: Should a dispute arise with the customer (dispute period) or a required retention duration (e.g. 5 years from when the account is closed).

Intermediate archive: This storage starts when the data is no longer used frequently but when the party that collected it or handles it may still need it to respond to a legal challenge or to comply with a statute of limitations.

**Restriction on access to data is required to reinforce data security and confidentiality.**

PD = Personal Data