POWER DESIGN

# GDPR and Data Protection Policy Statement

# GDPR AND DATA PROTECTION POLICY STATEMENT

## 1 Introduction

As a Data Controller, Power Design and its staff (hereafter referred-to collectively as PDA) comply with the Data Protection principles set out in the relevant Irish legislation. A substantial proportion of the communications sent by PDA to organisations is considered 'business to business', and thereby exempt from obligations under the Data Protection legislation.

Electronic and non-electronic communications of this nature by PDA are only to non-individual, business contacts and institutional subscribers. These come in the form of hard-copy mailings and e-mails. Hard copy mailings go to business/company addresses while business subscribers receive electronic mailings through their company email addresses.

In its role as an employer, PDA may keep information relating to a staff member's physical, physiological or mental well-being, as well as their economic, cultural or social identity.

To the extent that PDA's use of personal data qualifies as 'business to customer' processing, including the organisation's communications to its staff and clients, the organisation is mindful of its obligations under the relevant Irish legislation, namely:

- The Irish Data Protection Act (1988);
- The Irish Data Protection (Amendment) Act (2003); and
- The EU Electronic Communications Regulations (2011).

### Environmental changes that may affect the quality of data

The PDA policy is to be aware of environmental changes that affect the quality of data and to pre-empt the impact to our business and that of our clients. GDPR was the most recent change, one that we had spent two years preparing for. This meant that we had cleansed our databases and remodelled our business processes well ahead of the May 2018 deadline, enabling us to continue without any loss of continuity to our business.

### PDA as a Data Controller

In the course of its daily organisational activities, PDA may acquire, process and store personal data in relation to living individuals. To that extent, PDA is a Data Controller, and has obligations under the Data Protection legislation, which are reflected in this document.

In accordance with Irish Data Protection legislation, this data must be acquired and managed fairly.

PDA is committed to ensuring that all staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer (DPO) is informed, in order that appropriate corrective action is taken.

Due to the nature of the services provided by PDA, there is a regular and active exchange of personal data between PDA and its Data Subjects. In addition, PDA

exchanges personal data with Data Processors on the Data Subjects' behalf. This is consistent with PDA's obligations under the terms of its contracts with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

## The Data Protection Principles

The following key principles are enshrined in Irish legislation and are fundamental to PDA's Data Protection policy. In its capacity as Data Controller, PDA ensures that all data shall:

- Be obtained and processed fairly and lawfully.
- Be obtained only for one or more specified, legitimate purposes.
- Not be further processed in a manner incompatible with the specified purpose(s).
- Be kept safe and secure.
- Be kept accurate, complete and up-to-date where necessary.
- Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.
- Not be kept for longer than is necessary to satisfy the specified purpose(s).
- Be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.

## Data Subject Access Requests

As part of the day-to-day operation of the organisation, PDAs staff engages in active and regular exchanges of information with Data Subjects. Where a valid, formal request is submitted by a Data Subject in relation to the personal data held by PDA which relates to them, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which PDA must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

PDA's staff will ensure that such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 calendar days from receipt of the request.

## Implementation

As a Data Controller, PDA ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation through the Data Processor Agreement. Regular audit trail monitoring is done by the Data Protection Officer to ensure compliance with this Agreement by any third-party entity which processes Personal Data on behalf of PDA. Failure of a Data Processor to manage PDA's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts. Failure of PDA's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

# 2 Data Storage & Archiving

The following policies apply to company computer, server and database:

- PDA only provide limited access to personal data on a need to know basis
- Servers including the database server for hosting web content, web services and personal or non-personal data is within the PDA Computer Centre (CCC) with a specific IP address in Ireland.
- The CCC is managed by a trusted IT operator with SLA.
- Any access to the computer systems is monitored and logged on a 24/7 basis. The log includes the username, access time and duration.
- Computing devices, including PC, laptop, or mobile phones etc are located within the Company office (with a specific IP address). Each device is protected by a unique password and have one designated owner. On a shared device, each user has their own unique password for access.
- All computing/storage devices in the company and office are equipped with anti-virus software and protected with firewall. Unattended devices are locked automatically with a screen saver.
- PDA maintains a list of restricted databases and application along with a defined business owner for each listing. Only the account (contract) manager can authorize an individual to have any access to the restricted database or applications.
- Unescorted access is restricted to authorised persons for valid and documented business purposes.
- Visitors to the company or area for above infrastructures must be escorted by authorised staff, and their access must be logged with the visitor identity, time in and time out and reason for entry. This information is maintained in a central record system for one year.
- Email attachments from unexpected sources are not be opened unless first screened by anti-virus software.
- All data provided to us for mailing/distribution, is destroyed and certified on completion of a project.

## Network Infrastructure

- Staff can access the Company network inside the office. Remote access is only allowed with prior authorisation.
- Modems must be locked in a case and the key removed and secured.
- The Company WIFI network is protected by password.
- LANs shall be designed so as to limit the aggregation of data subject to unauthorised interception.
- Active ports are not allowed on network backbones unless the port is located in the Company Computer Centre
- If a data port is located in the Company Public Space (e.g. reception), it must be supervised at all times while it is active.

## Storage and Archive

- Contents, web services and database are hosted and stored on designated Company storage servers, not on any local devices.
- If downloading of personal data from above servers is necessary for data processing, such downloading can easily be blocked by technical means (disabling drives etc). Also, the downloaded data must be deleted immediately after the data processing.
- Content, web services and database are backed up automatically on a daily basis.
- Content, web services and database are archived from backups and retained for 1 year.
- Storage backup media are stored in the Company Computer Centre at all times.
- All databases including backups are in encrypted format and protected by password.
- Records of data wiping are stored electronically in the central record system.
- Cloud based or file sharing systems are only used when agreed with all parties and data files should be password protected and removed once transfer is completed.