PDW Group (UK) Limited

Data Protection and Data Security Policy

Policy Created: 15th March 2018 to comply with EU laws and the G.D.P.R.
Policy Updated: 31st March 2022

Statement of policy and purpose of Policy

1. PDW Group (UK) Limited (the Supplier) is committed to ensuring that all personal information handled by us will be controlled and processed according to legally compliant standards of data protection and data security, including the latest EU legislation and the GDPR.

2. PDW Group (UK) Limited is registered with the Information Commissioner's Office (ICO) with registration number Z1901931

3. The purpose is of this policy is to help us achieve our data protection and data security commitments by:

a. notifying our clients (which include decision makers, training delegates, software users, venue delegates, visitors and survey participators) prospects and website visitors **(collectively referred to as Clients)** of the types of personal information that we may hold about them, where and how we hold it and what we do with that information;

b. ensuring our employees understand our rules and the legal standards for handling personal information relating to the above groups: and

c. clarifying the responsibilities and duties of our employees in respect of data protection and data security.

4.This policy states our commitment around the cornerstones of the GDPR which include:

a. What personal data relating to a living individual do we keep in electronic or hard copy format?

b. What consents we have to keep that information

c. Our policy of deleting data

d. How have we explained what we do with the data

e. What data can be anonymised and what data cannot

f. Providing we have consent whether we need to keep the data and if so for how long

g. How and where we store the data and any risks associated with keeping it

h. How we are minimising those risks

Who is responsible at PDW Group for data protection and data security?

5. Maintaining appropriate standards of data protection and data security is the duty of all directors, employees, contracted consultants and agency workers. **(Collectively referred to as 'employees')**

6. The board of directors of the Supplier has overall responsibility for ensuring that all personal information is handled in compliance with the law and has appointed a Board Director as the Data Protection Officer with day-to-day responsibility for data processing and data security.

7. All employees have personal responsibility to ensure compliance with this policy, to handle all personal information consistently with the principles set out here and to ensure that measures are taken to protect the data security. Senior Management Team members have special responsibility for leading by example and monitoring and enforcing compliance.

8. Any breach of this policy will be taken seriously and may result in internal disciplinary action.

What personal information and activities are covered by this policy?

9.This policy covers personal information:

a.which relates to a living individual who can be identified either from that information in isolation or by reading it together with other information we possess;

b.is stored electronically or on paper in a filing system;

c.in the form of statements of opinion as well as facts;

d.which relates to Clients or to any other individual whose personal information we handle or control;

e.which we obtain, hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.

Data Protection Principles.

10. As a principle, the Supplier will comply with the eight legal data protection principles which require that personal information is:

a. **Processed fairly and lawfully.** We must always have a lawful basis to control or process personal information. In most (but not all) cases, the person to whom the information relates (the **Subject**) must have given consent. The Subject must be told who controls the information, the purpose(s) for which we are processing the information and to whom it may be disclosed.

b. **Processed for limited purposes and in an appropriate way.** Personal information must not be collected for one purpose and then used for another. If we want to change the way we use personal information we must first tell the Subject.

c. **Adequate, relevant and not excessive for the purpose.**

d. **Accurate.** Regular checks must be made to correct or destroy inaccurate information.

e. **Not kept longer than necessary for the purpose.** Information must be destroyed or deleted when we no longer need it. This document sets out later on how long we keep all different types of information.

f. **Processed in line with Subjects' rights.** Subjects have a right to request access to their personal information, prevent their personal information being used for direct- marketing, request the correction of inaccurate data and to prevent their personal information being used in a way likely to cause them or another person damage or distress.

g. **Secure.** See further information about how we keep data secure later in this document

h. **Geographical boundaries.** Not transferred to people or organisations situated in countries without adequate protection, and not outside the EU unless organisations outside of the EU can demonstrate compliance to the GDPR

11. Some personal information needs even more careful handling. This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life or about criminal offences. Strict conditions apply to processing this sensitive personal information and the Subject must normally have given specific and express consent to each way in which the information is used.

What personal information do we hold or process about Clients, in what capacity and what do we do with it?

12. We collect personal information about you which:

a. you provide, a key contact at your organisation provides on your behalf, or we gather before or during your engagement with us;

b. is in the public domain.

13. The types of personal information that we may collect, store and use about you will vary depending on your relationship with us as shown below. We will only collect, store or use information for the specific purpose and in the specific capacity it was intended, and will not 'swap' data from one purpose and capacity to another, without first obtaining your consent.

a. **Client decision makers** – in addition to your name and work email address, it is likely we will hold a work postal address, job title, work phone numbers and any personal interests which may have come up in conversation with us

b. **Training workshop delegates' written content** – in addition to your name and work email address (which may be provided to us by someone else at your organisation) it is likely we will hold your phone numbers & job title. We will also hold whatever information you choose to input into our My Learning Journey web portal, the purpose of which is to maximise your training experience with us. This information may be the types of scenarios you want to work with us on, specific personal scenarios that you are concerned about that you want to improve at, your work objectives and targets, and specific activities and plans you have to apply your learnings with us

c. **Training workshop delegates video footage** – if your training event with us is held at our Nottingham based Development Centre, it is likely (unless you have expressly asked us not to) that we will record your individual behaviour and coaching sessions with our consultants and will hold that video footage on your behalf to enable us to provide this footage if you request it. The amount of time we hold it depends on whether you make us aware that you require a copy or not (see later section on how long we keep your data for)

d. **Users of PDW Group SaaS (Software as a service) and bespoke software applications -** if your company uses (and has an agreement to use) a software application supplied by us, and you are a self-service user of that software, it is likely that your name and email address (which could be a work or a personal email address) will be (or will have been) supplied to us by a key decision maker or administrative contact at your company in order to enable us to set you up on the system and for you to use the software. It is then entirely your choice as to what information over and above your name and email address you input into the system (although your company policy may seek to override this and instruct you to add in data to some fields). The data fields available include but are not limited to:

i. Home address, personal contact details, date of birth, gender and nationality
ii. National insurance number
iii. Pay and benefits received as part of your employment

iv. Training attended and qualifications achieved, including a personal development plan

v. Records for disciplinary and grievance

vi. Any company assets which have been allocated to you

vii. Your access level

viii. Risk assessments, and accident records

ix.Your targets and work objectives

x. Feedback about you given from other colleagues, or given by you to other colleagues

xi. Formal and informal reviews completed by you and/or your line manager

xii. Bank details (these details are encrypted)

xiii. Disability, religion, ethnicity & sexual orientation

xiiii. Miscellaneous notes

e. **Our SaaS products** provide some data fields that are considered sensitive, such as religion, ethnic origin and sexual orientation. The Supplier does not in any way control this data and users have full choice as to what information they input. These fields are provided because many companies want to track the demographic data for their workforce

f. **Feedback providers for participation in an online or telephone survey initiative** – If you are a participator in a client (external) or employee (internal) survey requested by our Client and administered by us, it is necessary that our Client provides us with as a minimum your name and email address so we can instigate the survey. Depending on the type of survey, we may then also obtain from our Client the following data i. Customer feedback surveys (external) – market sector, gender, geographical region ii. People engagement surveys (internal) – job grade, department, location, gender, length of service. For 360 feedback surveys there is no further demographic data gathered. Whilst this data held is personalised, it is reported on anonymously.

g. **Users of our secure file transfer system** – we use our secure file transfer system where personal data or sensitive company data needs to change hands between PDW Group and a second party securely as using email across networks is not considered secure. We use this for two purposes:

i. Where we need to pass personal data to an individual or stakeholder who is a client or other stakeholder for the purposes of us carrying out the agreed business with them

ii. Where an individual for themselves or on behalf of their organisation wishes to pass personal data to us for the purposes of us carrying out the agreed business with them

h. **Visitors to our Development centre** – all visitors to our centre (suppliers, delegates, venue delegates, etc) are expected to sign in, and this is done via an iPad using a signing in App called Envoy. This App collects name and email address, and asks for consent to be added to any marketing mailing list that we have. The data for this App is stored within the EU.

i. **Visitors to our website**. There is a separate and already published PDW Group website privacy and cookies policy. This is accessible via our website at https://www.pdwgroup.co.uk/privacy-and-cookies

j. **Contact via our website**. The supplier provides a simple 'Contact Us' enquiry form on the 'Contact Us' page of the website at https://www.pdwgroup.co.uk/contact-us. For any user wanting to contact us via the website, they are asked for their name** and company name, email address**, telephone number and a brief overview of the nature of their enquiry. Those fields with a ** are mandatory. This data is stored in a separate database which is hosted by our website provider, WP engine who have confirmed they are fully compliant with our data protection policy. Users are required to give their consent for us to be able to add them to our marketing database.

14. We will use this information to carry out our business, to administer our relationship with you, to ensure we provide high levels of service to you and to resolve any problems or concerns you may have including but not limited to:

a. Opinions about other people or your organisation that you may have inputted into one of our online surveys that you want to remain anonymous

b. Personal feelings and development areas (including such items as a 360 feedback report that you may have inputted or uploaded)

c. Personal or even sensitive data that you may have inputted into one of our HR software applications

d. Copies of video film footage of you which have been recorded at our Nottingham Development Centre for developmental purposes which contains sensitive or personal content, conversations or behaviour.

15. We confirm that that for the purposes of the GDPR 2018, the Supplier is both a Data Controller and a data Processor of the personal information in connection with your business with us as follows:

a. The supplier is a data controller for delegate video footage in a training workshop situation. This means that we determine the purposes for which, and the manner in which, your personal information is processed.

b. The supplier is a data processor for all other situations specified in section 13. This means that we merely process or provide a vessel to hold the data for a specified purpose and do not determine the purpose or the manner in which your personal information is processed.

16. We use sub-processors where needed to assist us with processing client and user data. We only use sub processors that are GDPR compliant which are either in the EU or are not but have formally agreed to the ICO's standard GDPR clauses. A list of sub processors we use is below including the relevant web links so you can confirm their agreement to the standard clauses.

Sub Processor	Purpose	Region	Agreed to ICO Clauses?	Web Link
Amazon Web Services EMEA SARL	Primary cloud infrastructure	Luxembourg	Yes	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
Functional Software, Inc.	Application error monitoring	United States	Yes	https://sentry.io/legal/dpa/2.0.0/
The Rocket Science Group LLC	Email Service Provider	United States	Yes	https://mailchimp.com/legal/data-processing-addendum/
Freshworks, Inc.	Customer Support	United States	Yes	https://www.freshworks.com/data-processing-addendum/
Hotjar Ltd	Analytics and User Feedback	Malta	Yes	https://hotjar.eu1.echosign.com/public/esignWidget?wid=CBFCIBAA3AAABLblqZhB24Pf0StieMUYoPhZjLSQREW72TWQoLK6pAinYy2zbB8uczxUqeZDdERVruVZ_y6c*
Atlassian, Inc.	Application Development	United States	Yes	https://www.atlassian.com/dam/jcr:a7be1b13-555e-4ba6-9579-0f3cb83ee123/Atlassian%20DPA%202020%2010%2012.pdf
Slack Technologies Limited	Internal Communication	Ireland	Yes	https://slack.com/intl/en-gb/trust/compliance/gdpr
Google LLC	Document Storage, Analytics, Customer Support	United States	Yes	https://privacy.google.com/businesses/processorterms/
Stripe, Inc.	Billing and Payment Processing	United States	Yes	https://stripe.com/dpa/legal
WPEngine, Inc	Contact forms	United States	Yes	https://wpengine.com/legal/dpa/
Bullet Train Ltd	Feature management for web apps	United Kingdom	Yes	https://flagsmith.com/privacy-policy/
Backblaze	Secondary storage provider for back ups	Netherlands	Yes	https://www.backblaze.com/company/dpa.html
Envoy	Visitor sign in at to PDW Centre	United States	Yes	https://envoy.com/security-details/#privacy
Cloudflare, Inc.	Security and performance cloud	United States	Yes	https://www.cloudflare.com/en-gb/cloudflare-customer-dpa/

17. If you consider that any information held about you is inaccurate then you should tell us in the first instance by emailing us at hello@pdwgroup.co.uk. If we agree that the information is inaccurate then we will correct it. If we do not agree with the correction then we will note your comments.

18. We will take reasonable steps to ensure that your personal information is kept secure, as described later in this policy and in general, we will not disclose your personal information to others outside the Supplier. However, we may need to confirm to a key contact within our Client what specific information is held about specific delegates or users

19. By providing your personal information to us, you consent to the use of your personal information (including any sensitive personal data) in accordance with this policy.

What Consents do we have and how do we obtain them?

20. The Supplier will always ask for consent to obtain, hold and use your data, either directly from you or from a nominated representative from your company on your behalf whether this company is your employer or your supplier. Specifics on how we obtain consent from you or our Client depending on your relationship with us are:

a. **Client decision makers** – as a person of authority, and likely to be a key contact for the Supplier, you can decide what you send to us, what you upload (or authorise to be uploaded) to us, or what you input yourself into any of our software applications

b. **Training workshop delegates' written content** – with the exception of your name and email address (which is likely to be supplied to us centrally by a representative of your company) you can opt to give or not give your consent for keeping your data when first logging in and accessing our My Learning Journey Portal. This is done via an automated box which has both a link to this policy as well as a button to authorise consent which appears on first login. If you do not give consent in this way, then you cannot input any further information into the portal. Even if you have technically given 'consent' by clicking this button, any information you input is entirely voluntary and so you can opt to input all, some or none of the information being requested

c. **Training workshop delegates video footage** – if your training event with us is held at our Nottingham based Development Centre, it is likely (unless you have expressly asked us not to) that we will record your individual behaviour and coaching sessions with our consultants and will hold that video footage on your behalf to enable us to provide this footage if you request it. If you do not wish us to record your activity and therefore do not give us your consent, then you can do this either via phone or email to the relevant lead facilitator prior to attending your event with us, or by telling the lead facilitator on the day, before any recording begins.

d. **Users of PDW Group SaaS (Software as a service) and bespoke software solutions** – if your company uses (and has an agreement to use) a software application supplied by us, and you are a self-service user of that software, it is likely that your name and email address (which could be a work or a personal email address) will be (or will have been) supplied to us by a key decision maker or administrative contact at your company in order to enable us to set you up on the system and for you to use the software. It is then entirely your choice as to what information over and above your name and email address you input into the system (although your company policy may seek to override this and instruct you to add in data to some fields). If you do not consent to some or any of the information being held within this software, you simply do not input it. If it has been inputted on

your behalf by someone at your company, then in some cases you can delete it yourself, or if not, you should contact the appropriate person in your company to arrange for it to be deleted.

e. **Feedback providers for participation in an online or telephone survey initiative** – if you are a participator in a client (external) or employee (internal) survey requested by our Client and administered by us, it is necessary that our Client provide us with as a minimum your name and email address so we can instigate the survey. You do not need to complete the survey if you do not wish to, and so consent is essentially given by you completing the survey or not.

f. **Our secure file transfer portal** – all users are requested to consent to our data protection policy & its usage terms and conditions prior to using the portal. All data uploaded from an outside party to PDW Group belongs to the originator and not to PDW Group. Whilst the security of the supplied data is covered by this policy, PDW Group accepts no liability for any information or data uploaded to the our secure portal and accepts no liability for fraudulent, inaccurate or inappropriate information received.

g. **Visitors to our Development centre** – all visitors to our centre (suppliers, delegates, venue delegates, etc) are expected to sign in, and this is done via an iPad using a signing in App called Envoy. This App collects name and email address, and asks for consent to be added to any marketing mailing list that we have. The data for this App is stored within the EU.

What is our policy on deleting data?

21. The Supplier will not hold and store your data for any longer than is necessary to provide the expected level of service to you and the Client, and to minimise data protection risk to all parties. Specifics on how long we will keep data and how we will dispose of it depending on your relationship with us are:

a. **Client decision makers** – we will retain your name, email address and contact details in our web based CRM system for as long as you are a prospect or a client of the Supplier. Once you have formally told us that you no longer wish to be a Client of PDW Group then we will delete all your data records from our databases.

b. **Training workshop delegates' written content** – we will retain your name and email address, and any inputted content by you for the duration of you being an 'active' delegate on a PDW Group training or coaching programme. The definition of 'active' may extend beyond the completion of the formal programme as it may be important to you that we retain your records for ongoing access, development plan purposes and for future programmes with us. If you formally request us to delete your records, we will do so.

c. **Training workshop delegates video footage** – unless you have expressly not given us your consent to record your scenario based activities, we will digitally record the 1:1 and group sessions held at our Nottingham based Development centre. Our recording equipment typically stores all film footage for a period of up to 20 days if on regular record, where it then overwrites all previous footage automatically. In a particularly quiet phase it may be that we retain your footage for up to

60 days. If you do not request any copies of your film footage then your video data will be deleted no later than 60 days from the date it was recorded. If you do request a copy of one or more of your sessions with us, then we will make a copy and upload it to YouTube viewable only by you via a private URL. You can then choose who to share that link with. If you choose this option, the video footage is kept live for as long as you want access to it. If you wish us to delete it, you can email us at hello@pdwgroup.co.uk and will do so immediately.

d. **Users of PDW Group SaaS (Software as a service) and bespoke software applications** – if your company uses (and has an agreement to use) a software application supplied by us, and you are a self-service user of that software, you will have been added into the system as a user by either yourself, or a representative from your company. If you do not wish to be a user of the system then you should contact the relevant person at your company (the Client) to arrange for your basic details to be deleted. If you are leaving the employment of the Client then it is the responsibility of the Client's administrators as the data controllers to decide when user data is deleted from the system. Where the Client formally serves notice to the Supplier to terminate the contract for SaaS, all primary system data will be automatically deleted from our servers at the six month point after system access has been stopped. Data backups however will auto delete over time to our backup schedule shown on page 14.

e. **Feedback delegates & providers participating in a 360 degree feedback initiative** - – if you are a participator (delegate or provider) in a 360 degree feedback survey requested by our Client and administered by us, it is necessary that our Client provides us with as a minimum your name & email address so we can instigate the survey.

i. **Participant data** - Participant data is only supplied to us via our own secure document portal; we do not accept it via email. This data automatically deletes 3 months after it was uploaded unless the client requests in writing that it be retained by us for longer.

ii. **Survey response data** – this data is a series of in-depth quantitative scores and qualitative comments made by participants about an individual. This data is considered personal data as it is associated with the recipient (the delegate) even though it is typically provided by others anonymously by others. This data is held within our online 360 feedback system and is not deleted as it is often required to assist our clients with reporting on performances as well as comparison data for instance year on year. If one of our Clients or delegates wishes us to delete the 360 feedback report, then we will do so as soon as we are contacted.

f. **Feedback providers for participation in an online or telephone employee or customer survey initiative** – if you are a participator in a client (external) or employee (internal) survey requested by our Client and administered by us, it is necessary that our Client provides us with as a minimum your name and email address so we can instigate the survey.

i. **Participant data** - Participant data is only supplied to us via our own secure document portal; we do not accept it via email. This data automatically deletes 3 months after it was uploaded unless the client requests via the portal that it be retained by us for longer.

ii. **Survey response data** – this data is a series of in-depth quantitative scores and qualitative comments made by participants. This data for internal employee surveys is often reported anonymously and so is not considered personal data; for customer surveys it is typically reported personally. Once the Supplier has collated all the data and the survey end date has passed, the Supplier provides the data in a PDF report format which is then provided to the Client. Increasingly, the same data is held digitally for as long as the Client requires it, and as with all data, is deleted immediately if the Client requests it.

g. **Secure file transfer**

i. **Documents received by PDW Group**: we will delete all data and documents uploaded to our secure file transfer system by an authorised user automatically after three months from the date it was uploaded except where the originator has expressly requested us to either delete it sooner, or to keep it for longer.

ii.**Documents sent/uploaded by PDW Group**: we will delete all data and documents uploaded to our secure file transfer system by PDW Group automatically after three months from the date it was uploaded except where the recipient has expressly requested us to either delete it sooner, or to keep it for longer.

22. The Supplier stores very few hard copy documents containing any personal data; most personal data is stored digitally as referred to in section 2

23. Any personal data stored in hard copy will be stored securely & shredded to comply with any deletion request.

What Are the Risks to Your Personal Data?

24. The keeping, holding, processing and using of any personal data is not without risk. See below for how The Supplier will minimise those risks and ensure your data is protected.

25. The risks which we have identified, which are the same for any business of our type are:

a. Physical documents being left unattended and obtained or seen by unauthorised individuals

b. Physical servers or other computer hard drives containing personal data being damaged by fire or flood, or stolen from the premises

c. Personal data being supplied by our Client and one or more employees, users, delegates or participants (depending on the purpose of the data and the service being supplied) feeling they do not have control or feel they have not consented to their information being held or used.

d. Data being corrupted, infected, lost or stolen and getting into the wrong hands

e. Software systems being unlawfully accessed by unauthorised users

f. Software users allowing their usernames and passwords to get into the wrong hands and be

accessed by unauthorised persons

g. Data being stored for longer than is necessary, required or beyond the time boundaries as specified in this policy. Data not being deleted if it is requested to be deleted by the Client.

h. Data being stored and claimed as anonymous when it is not, and specific persons can be identified

i. Data not being backed up as it should be and therefore being lost or irretrievable

j. employees of the Supplier not being sufficiently trained to allow them to properly enforce this data protection policy in full

k. employees of the Supplier who are not authorised to access or use certain types of instances of personal data being able to access it either by accident or on purpose

l. Data being held or sent outside of the EU where the level of data protection law may not be to the standard of the GDPR

How Do We Ensure Data Security and Minimise the Above Risks?

26.The Supplier must always protect personal information in its possession from being accessed, lost, deleted or damaged unlawfully or without proper authorisation through the use of data security measures.

27. Maintaining data security means making sure that:

a.only people who are authorised to use the information can access it;

b. information is accurate and suitable for the purpose for which it is processed; and

c. authorised persons can access information if they need it for authorised purposes. Personal information therefore should not be stored on individual computers but instead on our central system.

28. By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying it.

29. Personal information must not be transferred to any person to process (e.g. while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

30. Our security procedures include but are not limited to:

a. **Physically securing information.** Any desk or cupboard containing confidential information must

be kept locked. Computers should be locked with a password or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others. We have no physical on site servers, all information is stored on off site cloud based servers.

b. **Controlling access to physical premises.** The front doors to the Supplier premises are locked and alarmed when not attended, and always manned during office hours. There are also key card entry systems on both main internal doors to the main employee areas of the building and no one other than PDW employees and formal contractors are issued with a key card. employees should report to the office manager if they see any person they do not recognise in an entry-controlled area.

31. **Telephone & Email Precautions.** Particular care must be taken by employees who deal with telephone enquiries and may receive bogus emails to avoid inappropriate disclosures. In particular:

a.the identity of any telephone caller must be verified before any personal information is disclosed;

b.if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;

c.do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the Data Protection Officer.

d. Any email that is received by any employees member where the identity of the sender cannot be verified, and the safety of the contents, links or attachments cannot be guaranteed is not opened and is deleted from our server.

32. **Methods of disposal/deletion.** Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs, memory sticks including backups must be fully deleted and rendered permanently unreadable.

33. **Sending data to others**. No personal data is sent from the Supplier to an outside recipient via email or unsecured digital means.

34. **Employee training.** All employees on joining the Supplier's employ attend an in depth training session on this policy and their role in ensuring it is delivered and adhered to in full. All current employees are expected to attend and sign to confirm attendance at a training session for major policy and legislative changes such as the GDPR.

35. **Digital storage.** There are a number of security features that we have invested in to assist in the physical and technological protection of your data held digitally. These include:

a. All our latest software systems, both SaaS, our survey portals and our My Learning Journey portal has been built to the latest standards in web security and all demonstrate multiple levels of protection against SQL injection and unauthorised access. We have either deleted, transferred or stopped using any previous software versions of these applications where we are not confident of the security levels

b. All our customer data is transferred securely using HTTPS (encrypted SSL connection) from the Client browsers to our servers.

c. All our web portals are built using the same technology and coding principles and although we have not penetration tested every system, we have penetration tested these principled applications to ensure they can withstand attempts to gain unauthorised access

d. Sensitive data such as bank details are encrypted on our SaaS products

e. Data is stored wherever possible in the Cloud, using high quality storage companies who take data protection seriously, such as Amazon Web Services (AWS).

f. Master login details for all PDW internal, client and third party software applications are held securely in a Lastpass web portal. Lastpass is a highly secure third party password repository which has a complex master password only known to select PDW employees on a 'need to know' basis.

g. All data that we hold, control or process is done so within the EU. All data is held on UK based servers and is never 'sent' and downloaded onto hard drives which are not physically present in the EU and are therefore under EU law. The only exception to this is our use of sub processors who choose to store their data outside of the EU but have all confirmed agreement to the ICO standard clauses and as such are compliant with the GDPR. A list of these sub processors is shown on page 7 of this document.

36. **Data Backup.** The Supplier operates a stringent back ups policy which includes the following components and commitments:

The below covers our Immerse Works People Software, most Client specific bespoke web systems, our My Learning Journey web system, 360 Feedback & Feedback Services portals.

a. Data is backed up three times per day to cloud servers and these are kept for the first seven days. Back ups are then stored to the following schedule:

i. Once daily backups are kept for the last 16 days

ii. Weekly backups are kept for the last 8 weeks

iii. Monthly backups are kept for the last 4 months

iv. Annual backups are kept for two years

b. Data back ups are held in two remote cloud based locations with two seperate companies, Amazon Web Services and Backblaze. We have a backup data storage limit of 200GB for Immerse Works, and 100GB of data covering all other systems, per provider. If/when either of these limits are reached, the oldest backup data will be automatically overwritten/deleted.

c. Backed up data is encrypted with encryption keys stored in our in house password repository. Encryption keys are rotated every half year.

d. We have enabled daily whole-server snapshots for a rolling seven day period which enables rapid restoration of an entire server in the event of a ‘crash’

e. Accidental file deletion recovery & ransomware protection is incorporated into our cloud storage

37. **Wi-fi Network**. The Supplier has a split wi-fi network at our Nottingham Development Centre, one which is password protected with only employees being issued the password. The other is for clients and visitors where the password is available internally within the building.

38. **Suspected data breaches.** If we become aware of any suspected or actual breaches and access has been gained by unauthorised users, we will immediately take that application off line, and seek to understand the nature of the issue. We will then not put the application back on line until the issue has been fixed and full data security can be confirmed.

a. If a data breach has been confirmed, we will inform you and we will report this to the ICO including a full report on what data is at risk, and the circumstances surrounding the breach.

Subject access requests

39. By law, any Subject (including employees) may make a formal request for information that we hold about them, provided that certain conditions are met. The request must be made in writing either by post, email or other electronic means. There is no fee payable for this service unless the request is manifestly unfounded or excessive. In some circumstances it may not be possible to release the information about the Subject to them e.g. if it contains personal data about another person.

40. Any member of employees who receives a written request should forward it to the Data Protection Officer immediately.

For further information regarding this data protection policy, please contact:

The Data Protection Officer
PDW Group (UK) Ltd, Units 9a-9c, Colwick Quays
Business Park. Colwick. Nottingham NG4 2JY
Telephone: 0115 940 4966
Email: hello@pdwgroup.co.uk

ICO registration number: Z1901931