PayDashboard Privacy Notice

In addition to adhering to the above principles, when acting as a Data Processor in relation to your Personal Data, we shall act in accordance with the instructions provided to us by your employer (the Data Controller).

Personal Data

1. The Personal Data, as defined under the GDPR, which we process in accordance with the instructions of the Data Controller, includes certain information which can be used to identify you.

2. Although we do not actively collect and/or process Special Categories of Personal Data your employer may decide to provide such data (such as trade union membership) for us to process. Should the service change to actively collect and/or process Special Categories of Personal Data, we shall inform you, as well as any further protections that we may implement.

3. The Personal Data we collect and Process about you is as follows:

Types of Data

Our Capacity	**Data Processor**
Purpose/Activity	To provide access to your employer to publish payroll-related data and employee benefits related data. To provide pay related documents as defined by payroll processing legislation. To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking to leave a review or take a survey. To deliver notifications to you about your payslip data. To deliver rewards functionality. To deliver relevant educational content to you. To use data analytics to improve our products/services, marketing, customer relationships and experiences. To make suggestions and recommendations to you about relevant goods or services that may be of interest. To provide support of the product.
Type of Data	**PayDashboard Service** Contact: Email Address. Identity: Title, Forename(s), Surname, Employee Number, NI Number, Address, Gender, Telephone Number, IP Address. Other: Payroll information and rewards/benefits information.

When	Data is passed each time payroll information is passed to us, by the Data Controller or an agent of the Data Controller.
How Long	Data will be held unless your employer no longer uses our services, at which point the Personal Data shall be deleted or anonymised.
Lawful Basis	By Contract with the Data Controller or an agent of the Data Controller

Our Capacity	Data Processor
Purpose/Activity	To provide availability of the service in the case of damage, corruption, or service interruption.
Type of Data	**Database Backup** All relevant payroll information collected during the operation of the system.
When	On a continuing basis during the operation of the system
How Long	Database backups will be held for a maximum of 35 days before being deleted.
Lawful Basis	By Contract with the Data Controller or an agent of the Data Controller

Our Capacity	Data Processor
Purpose/Activity	Prevention, investigation, detection or prosecution of criminal offences.
Type of Data	**System** Logs IP Address, URLs visited within the platform.
When	Ongoing basis during system use.
How Long	Deleted/anonymised after a period of 14 months.
Lawful Basis	By Contract with the Data Controller or an agent of the Data Controller

Our Capacity	Data Processor
Purpose/Activity	**Application Audit Trail** Prevention, investigation, detection or prosecution of criminal offences Providing transparency for access and changes made regarding the Personal Data.
Type of Data	Contact: Email Address. Identity: Title, Forename(s), Surname, Employee Number, NI Number, Address, Gender, Telephone Number, IP Address. Other: Payroll information and rewards/benefit information
When	Ongoing basis during system use.
How Long	Deleted/anonymised after a period of 14 months.
Lawful Basis	By Contract with the Data Controller or an agent of the Data Controller

Our Capacity	Data Processor
Purpose/Activity	To provide Employee rewards, financial and mental wellbeing partners to You.
Type of Data	**Pay** Dashboard Services Limited Contact: Email Address
When	When you first sign-up for this facility.
How Long	For the period you are a user of this facility.
Lawful Basis	By Contract with the Data Controller or an agent of the Data Controller

Our Capacity	Data Processor
Purpose/Activity	Operational management of the platform
Type of Data	**Microsoft** Azure Application Insights Identity: IP Address Other: Site usage information including URL.
When	Ongoing basis during system use
How Long	Deleted after a period of 14 months
Lawful Basis	Legitimate Interest

Our Capacity	Data Processor
Purpose/Activity	Operational management of the platform to ensure the performance and capacity of the service meets service level agreement targets and the proper authentication of users to the service. To improve the service we provide by understanding how users engage with the service.
Type of Data	**Cookies** Identity: IP Address, Device ID, temporary unique user identifier Stored as cookies and other local storage mechanisms. See Cookies below.
When	Ongoing basis during system use and in-between sessions.
How Long	See Cookies below.
Lawful Basis	By Contract with the Data Controller or an agent of the Data Controller

Third-party links

1. Where we provide links to third-party websites, plug-ins and applications, clicking on those links or enabling those connections may allow third-parties to collect or share data about you. We do not control these third-party websites and we are not responsible for their privacy statements. We encourage you to read the privacy notice of every website visited.

Other Non-Personal Data

1. This is data where the identity has been removed (anonymised data). We use such data for our own purposes, as well as providing extracts of such information to third parties. Once personal data is anonymised it is no longer regarded as Personal Data, hence the GDPR no longer applies to that anonymised data.

Keeping in touch with you

1. We may keep you informed of the availability of the service or other relevant service-related notifications or new features and capabilities of the service.
2. We may keep you up to date with information about related services ("Marketing Information") we can offer either directly or through third-parties.
3. If you decide you do not want to receive this Marketing Information, you can request that we stop by the method we indicate to you.
4. We will not share your Personal Data with other companies other than as outlined herein.

Your Rights as a Data Subject

You have the following rights under GDPR:

1. the right to be informed, which encompasses the obligation to provide transparency as to how Personal Data will be used;
2. the right of access, otherwise known as a Data Subject Access Request (DSAR);
3. the right to rectification of data that is inaccurate or incomplete;
4. the right to be forgotten under certain circumstances;
5. the right to block or suppress processing of Personal Data; and
6. the right to data portability which allows you to obtain and reuse your Personal Data for your own purposes across different services under certain circumstances.

While we act as a Data Processor of your data, in order to exercise your rights under the GDPR you should contact the Data Controller, usually your employer. We shall then act upon the instructions of the Data Controller or such other party authorised to instruct us on behalf of the Data Controller.

Security of Data

1. We are committed to taking steps to ensure that Personal Data is protected, and to prevent any unauthorised access, unauthorised changes, accidental loss, destruction, unlawful processing, equipment failure or human error, and will do this through the continual monitoring of our security systems and by regular training and awareness raising.
2. Any data breaches will be managed according to the Company's procedures documented in its Incident Management Policy and Procedures.
3. Unless otherwise directed by legal obligation, any requests from a governmental body shall be referred to the Data Controller.

Other parties

In providing the Services, we currently engage the following parties as Data Processors, all of whom we have assessed to ensure compliance with the GDPR:

Processor	Service	Data	HQ
Microsoft Azure	Infrastructure hosting partner	UK	US
Mailgun Technologies (mailjet)	Email notification partner	EEA	EEA
Zendesk	Customer support ticketing partner	EEA	US
Google Analytics	Platform operational management partner	US	US
Forgerock	Identity access management	UK	UK
Esendex	Email and SMS provider for multi-factor authentication	UK	UK

Transferring Personal Data to a Country Outside the UK

1. Other than as set out above, we do not transfer Personal Data outside the United Kingdom (UK) if you are based within the UK.
2. If you are based outside of the UK, in order to provide our services, we shall be obliged to send the Personal Data outside of the UK, in order to reach you.
3. Whenever we transfer Personal Data out of the UK, in accordance with the above limited exception, we shall act strictly in accordance with the instructions of the Data Controller, where applicable.
4. Whenever we transfer Personal Data to a Data Processor outside of the UK, we have ensured that appropriate measures, as allowed for by the GDPR, are in place to continue the ongoing protection of the Personal Data. Such measures may include Standard Contractual Clauses, Binding Corporate Rules or Privacy Shield.

Data Protection Measures

We are committed to ensuring the security of Personal Data and to processing it in line with the Data Protection rules. As such, we will:

1. Ensure that all staff are aware of their responsibilities and our obligations and responsibilities in relation to data protection.
2. Ensure that all staff and individuals/organisations who handle data on our behalf are appropriately trained and receive refresher training on a regular basis.
3. Ensure that all staff and individuals/organisations who handle data on our behalf are regularly monitored, assessed and reviewed.
4. Ensure that all organisations who handle data on our behalf are carrying out data processing in line with the Data Protection rules.
5. Regularly review our methods of data collection, handling, processing and storage.

Monitoring

1. We are committed to monitoring this policy and will update it as appropriate, on an annual basis or more frequently if necessary.

Cookies and similar technologies

1. Cookies are small text files that your computer or mobile device downloads and stores on your browser when you visit a website. They allow the website or service to recognise the user's device and store some information about the user's preferences or past actions.

2. The service makes use of first party and third-party cookies to facilitate the operation and performance monitoring of the system and to provide a safe and reliable system. First-party cookies are set directly by the domain the user is visiting, i.e. the URL displayed in the browser's address bar. Third-party cookies are set by a domain other than the one the user is visiting.

3. The service makes use of Necessary cookies. These enable the core functionality of the service. They are essential and can only be disabled through changing your browser settings. If you do switch off these cookies in your browser, parts of the service may not work correctly.

4. We would also like to make use of optional cookies for security purposes and to help us improve the service we provide to you by understanding how users engage with the service. We will only make use of these cookies where you have provided us with your consent to do so.

5. As part of our service offering to improve the log-in experience, we will specifically ask for your permission to remember information about your device ID when you register for our services. By consenting to this, you are allowing us to store your device ID, which means you will not need to re-authenticate the next time you log in to the service. We will store your device ID details until you either 1) download the app on the new device 2) reset your multifactor authentication (MFA). To reset MFA, you will need to click on the reset icon on the top right-hand corner of the screen that asks for your authenticator code and you will then need to enter your National Insurance (NI)/ employee number/postcode to complete the reset.

6. We will also ask for your permission to collect web-platform analytics information to help us improve the service provided. We do this by collecting data about how you have interacted with the web-platform and mobile app. The data is collected in a way that does not directly identify anyone.

7. We do not use cookies for the purposes of direct marketing.

8. Cookies that are not persistent will be removed automatically at the end of your session with the service. Cookies that are anonymous cannot be used to identify you either during or after use of the service.

9. You can disable cookies by clearing your browser cache and cookies via your browser settings. You may need to refresh your page for your settings to take effect.

10. The table below explains the cookies we use and why.

Name	Provider	Purpose	Expiry	Type
__cfruid	Zendesk	This cookie is a part of the services provided by Cloudflare - Including load-balancing, deliverance of website content and serving DNS connection for website operators.	Session	HTTP Cookie
__mp_opt_in_out_#	cdn.mxpnl.com	Pending	Session	HTTP Cookie
__RequestVerificationToken	eecdev.paydashboard.com	Helps prevent Cross-Site Request Forgery (CSRF) attacks.	Session	HTTP Cookie
__zlcid	Zendesk	This cookie is necessary for the chat-box function on the website to function.	Session	HTTP Cookie
__zlcmid	Zendesk	Preserves users states across page requests.	1 year	HTTP Cookie
__zlcstore [x2]	eecdev.paydashboard.com Zendesk	This cookie is necessary for the chat-box function on the website to function.	Persistent	HTML Local Storage
__zlcstore	Zendesk	Necessary for the functionality of the website's chat-box function.	Session	HTTP Cookie
AI_buffer	Microsoft	Used in context with the "AI_sentBuffer" in order to limit the number of data-server-updates (Azure). This synergy also allows the website to detect any duplicate data-server-updates.	Session	HTML Local Storage
AI_sentBuffer	Microsoft	Used in context with the "AI_buffer" in order to limit the number of data-server-updates (Azure). This synergy also allows the website to detect any duplicate data-server-updates.	Session	HTML Local Storage
ASPXAUTH	eecdev.paydashboard.com	Identifies the user and allows authentication to the server	Session	HTTP Cookie

Name	Provider	Purpose	Expiry	Type
AWSALBCORS	Zendesk	Registers which server-cluster is serving the visitor. This is used in context with load balancing, in order to optimize user experience.	7 days	HTTP Cookie
CookieConsent	eecdev.paydashboard.com	Stores the user's cookie consent state for the current domain	1 year	HTTP Cookie
cookietest	eecdev.paydashboard.com	This cookie is used to determine if the visitor has accepted the cookie consent box.	Session	HTTP Cookie
incap_ses_#	paydashboard.com	Preserves users states across page requests.	Session	HTTP Cookie
UtcOffset	eecdev.paydashboard.com	Pending	Session	HTTP Cookie
visid_incap_#	paydashboard.com	Preserves users states across page requests.	1 year	HTTP Cookie
ZD-store	Zendesk	Registers whether the self-service-assistant Zendesk Answer Bot has been displayed to the website user.	Persistent	HTML Local Storage
zte#	Zendesk	Saves a Zopim Live Chat ID that recognises a device between visits during a chat session.	Session	HTTP Cookie

A. Standards Conformance

This document relates to the following clauses or controls in the following standards or regulations.

ISO 27001:2013: Information Security Management

Reference	Clause/Control
A13.2	Information transfer
A18.1.1	Identification of applicable legislation and contractual requirements
A18.1.3	Protection of records
A18.1.4	Privacy and protection of personally identifiable information

The General Data Protection Regulation

Reference	Clause/Control
Article 4(1)	Definitions
Article 5	Principles relating to processing of personal data
Article 6	Lawfulness of processing
Article 12	Transparent information, communication and modalities for the exercise of the rights of the data subject
Article 14	Information to be provided where personal data have not been obtained from the data subject
Article 15	Right of access by the data subject
Article 16	Right to rectification
Article 17	Right to erasure
Article 18	Right to restriction of processing
Article 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20	Right to data portability
Article 21	Right to object
Article 22	Automated individual decision making, including profiling
Article 25	Data protection by design and by default
Article 28	Processor
Article 29	Processing under the authority of the controller or processor
Article 30	Records of processing activities
Article 32	Security of processing
Article 33	Notification of a personal data breach to the supervisory authority
Article 34	Communication of a personal data breach to the data subject
Article 37	Designation of the data protection officer
Article 44	General principle for transfers
Article 45	Transfers on the basis of an adequacy decision
Article 46	Transfers subject to appropriate safeguards

13 December 2023
Version 2.4a

19 April 2024
Version 2.5

06 September 2024
Version 2.6

C-02412

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

www.experian.co.uk