Privacy Policy

Challenger is committed to protecting the privacy of all personal information collected in the course of business. Challenger complies with all data protection laws applicable to the United Kingdom.

This privacy policy applies to personal information about:

- visitors to the Challenger website – https://www.challengernw.co.uk;
- customers who purchase goods or services from Challenger;
- suppliers who supply goods or services to Challenger; and
- members of the public who have contacted Challenger.

For details on how Challenger may process the personal information of employees, job applicants, interns and volunteers, please see the HR Data Protection Policy in the HR Handbook, which is supplemental to this Policy.

This Policy explains how and why personal information is collected; who the information is shared with; why and on what basis; and what rights a person has with regards to their personal information.

Definitions

Personal information is any information that could be directly or indirectly used to identify a person. That could be anything from a name and address, bank details, email address, an image or recording, IP address or any other information that could be used to identify someone.

Personal information may include 'special category data' relating to racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, and criminal records and allegations.

'Processing' means doing something with personal information. That could be as straightforward as collecting it or sharing it, or as complex as modelling the information or appending values to the information.

Data controller and processor

Challenger is a data controller and as such is responsible for determining what happens to any personal information collected and how it is processed. Responsibilities also include monitoring and approving any data processors that the information is passed to.

Challenger may use data processors to provide personal information processing services. A data processor carries out processing on behalf of the data controller. As an example, Challenger (the data controller) may ask another company (the data processor) to store employee personal information in its cloud services. As a result, the data controller will provide the data processor with the personal information required to carry out this request without being able to control the personal information directly.

Processing of personal information

As a general rule, special category data about the persons covered by this Policy (as outlined above) is not collected. The exception is where suspected criminal activity is identified, such as, the use of stolen payment card details. In this case, all details of the suspected criminal activity (including any special category data) will be recorded, and appropriate action may be taken, including refusing to accept orders, make payments or give refunds. The incident may also be reported to the relevant bank or payment card issuer or to the police or other appropriate authority.

Personal information may be processed by Challenger in the following circumstances.

Contractors and consultants

Contractors and consultants working for Challenger may have their personal information stored and used:

- to assess their suitability during a tendering process;
- to comply with relevant laws and regulations;
- to arrange payment for goods and/or services;
- to communicate with the contractor or consultant;
- for record keeping purpose; and/or
- for claims management and insurance purposes.

Customers and prospective customers

Personal information about customers and prospective customers may be provided over the telephone, in person at our depot, via email, via our website or via our social media accounts.

If products or services are purchased or enquiries are made, personal information of customers or prospective customers may be stored and used to:

- respond to enquiries;
- keep customers informed about Challenger's products and services;
- process orders;
- follow up on orders that are not completed;
- process initial and ongoing payments for orders;
- manage deliveries and collections;
- manage a customer's account or credit account (if applicable) including carrying out trade references;
- deal with complaints;
- assist with claims management and insurance obligations;
- produce testimonials; and/or
- conduct market research.

In addition, Challenger may use the personal information collected from people who have previously signed up to a mailing list or have previously enquired or purchased products or services to let them know about similar products or services which may be of interest to them, and to keep them updated with information about promotional offers. Email or text marketing can be opted out of at any time by using the unsubscribe option in the message. Postal and/or telephone marketing can be opted out of at any time by contacting Challenger at the address at the end of this Policy.

Website cookies

The Challenger website can be visited and browsed without providing a name or contact details. However, like many websites, cookies are used to analyse how the site is used by visitors and to provide a more personalised online experience.

Cookies are a standard feature of most websites and allow small amounts of data to be stored on a computer. Cookies:

- help Challenger determine whether the website has previously been visited or not;
- make it easier to maintain preferences and enable certain features of the website to work;
- tailor information or adverts shown on the website to the individual browsing; and
- provide insights into which areas of the website are useful and which areas need improvement.

The Challenger website uses the following types of cookies:

- essential cookies – these are used to make sure the information is displayed correctly on the website, and they record whether or not additional cookies have been accepted;
- analytics cookies – Google Analytics is used to better understand: how visitors use the website; how users arrived at the website; how long users remained on the website; and whether users return to the website. They also help to control website traffic at busy times. These cookies use anonymous information only and are deleted after 26 months.
- functionality cookies – these are used to enable certain features of the website work such as email services, surveys, live chat features, contact forms, Google Maps and video.

Accepting cookies is a choice and this decision can be made and changed at any time using the settings on the user's web browser. However, disabling cookies can diminish the website experience and prevent features from working as intended. For details on how to accept, block and delete cookies you can use the 'help' feature on the web browser or visit http://www.allaboutcookies.org/. To opt-out of Google Analytics for the web, visit the Google Analytics opt-out page to install the Google Analytics opt-out add-on for your browser.

Suppliers

If products or services are supplied to Challenger, personal information of suppliers may be stored and used:

- for order processing and management;

- to manage deliveries/collections, installations, returns and refunds;
- to manage a Supplier's account, including conducting trade reference checks and other background checks, where applicable;
- for market research purposes;
- to notify Suppliers about important changes or developments to the website or services;
- for supply chain management;
- to deal with enquiries and complaints;
- for claims management and insurance purposes; and/or
- for record keeping purposes.

Members of the public (non-customers)

If contact is made with members of the public, personal information may be stored and used to deal with enquiries and complaints and for claims management and insurance purposes.

CCTV

A CCTV system is used within the offices, workshop and yard are. The CCTV system may be used to:

- ensure the safety and security of staff, buildings, assets and information located or stored on the premises;
- investigate security incidents, should such incidents occur;
- investigate breaches of policies and procedures or staff conduct or behaviour;
- monitor the progress of staff or individuals in the ordinary course of lawful business in the area under surveillance;
- observe staff working practices, time keeping or to assist in the day-to-day management of staff;
- ensure compliance with Challenger policies and procedures;
- capture images for training purposes; and
- in exceptional circumstances, where it is considered appropriate, the CCTV system may be used to visually monitor the health and/or behaviour of the staff.

The CCTV system will not be used for any other purpose without prior consultation with the Partners.

Challenger is committed to respecting people's rights to privacy and supports the individual's entitlement to go about their lawful business, although there will inevitably be some loss of privacy when CCTV cameras are installed. It is therefore crucial that serious consideration is given to the necessity for cameras in a given location. It is also essential that CCTV equipment is sited in such a way that it only monitors those areas intended to be covered. If it is not possible to restrict coverage of neighbouring spaces, the owner of a property or space being overlooked should be consulted. Cameras are not to be installed in such a way that they can look into private spaces such as toilets.

It is essential that legible 'CCTV Recording in Use' signs are displayed in a prominent place where CCTV

is in use and only where it is in use (except where 'covert' cameras have been authorised for deployment). The signs will act as an additional deterrent. All signs of this nature should have a yellow background with all writing in clear black print and should contain the following information:

- Challenger's name, as the entity responsible for the surveillance;
- the purpose of the surveillance;
- contact details of who to speak to regarding the CCTV; and
- an image of a camera.

CCTV recordings are only to be reviewed by Challenger Partners or members of the Management Team with authority from a Challenger Partner. Images provided to the Police or other enforcement agencies or for internal investigations shall at no time be used for anything other than the purposes for which they were originally released. All images will remain the property and copyright of Challenger. All media will be disposed of securely when no longer required.

Lawful basis for processing personal information

The specific grounds used for processing personal information depends on the nature of the processing. However, it is likely that the most applicable lawful basis for processing personal information in the circumstances outlined above would be that doing so is necessary to fulfil a contract between Challenger and a customer or supplier, or take steps at the request of the customer/supplier prior to entering into a contract. For example, Challenger may need to telephone an individual in response to a customer enquiry.

In other circumstances, the following lawful bases may apply:

- legitimate interest – processing personal information may be necessary for Challenger's legitimate interest in something;
- consent – Challenger may at times ask for an individual's consent to process their personal information; and/or
- legal obligation – in limited circumstances, Challenger may have a legal obligation to process personal information.

Security of personal information

Challenger is committed to safeguarding personal information that is provided in the course of business.

General security requirements

Employees handling personal information should ensure that they:

- keep passwords and accounts secure;
- do not install software or hardware, including modems and wireless access without explicit approval from a Partner;

- report any suspicious behaviour and/or breaches of this policy to a Partner without delay;
- exercise good judgment regarding the reasonableness of personal use of IT equipment;
- take all necessary steps to prevent unauthorised access to confidential data; and
- special care should be exercised when using information contained on portable computers.

Physical security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data. For example:

- visitors must always be escorted by a trusted employee when in areas that hold confidential data and information.
- a schedule of devices should be maintained. The list should include make, model, serial number and location of the device.
- personnel using the devices should report suspicious behaviour and indications of tampering of the devices to a Partner without delay.

Network security

The following network security arrangements are in place at Challenger:

- the allocation of privilege rights shall be restricted and controlled, and authorisation provided jointly by the system owner and IT services;
- access to confidential information will be limited to authorised persons whose job responsibilities require it;
- no external access for remote users shall be permitted to any network device or networked system without prior authorisation from a Partner;
- all data must be securely disposed of when no longer required by Challenger, regardless of the media or application type on which it is stored;
- Challenger will arrange for the destruction of hardcopy materials; and
- bulk download of personal information is not possible via Challenger IT systems without administrator access. All documents and files that are backed-up are encrypted.

Cardholder security

Challenger is transitioning to a new PCI compliant payments platform which allows payments to be processed without card details being visible by Challenger or any of its employees. This is the safest and most secure method that Challenger has identified to be able to process card payments for customers without taking card details over the telephone.

Until the old virtual terminal system is phased out, in order to prevent a breach of cardholder data or sensitive cardholder information Challenger and its employees will ensure that:

- all sensitive cardholder data stored and handled by Challenger and its employees must be securely protected against unauthorised use at all times;
- any display of the cardholder should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data;
- all sensitive cardholder data must be protected securely if it is to be transmitted. Cardholder data must never be sent over the internet via email, instant chat or any other end user technologies;
- all hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons; and
- all cardholder information awaiting destruction must be held in lockable storage containers clearly marked – access to these containers must be restricted.

It is also strictly prohibited to store the contents of the payment card magnetic stripe (track data), the CVV/CVC or the PIN or encrypted PIN block on any media whatsoever or in any circumstances.

Website security

Appropriate measures are used to protect the information that is submitted through Challenger's website as well as the information collected and stored about customers. Unfortunately, the transmission of information via the internet is not completely secure. Although personal information will be protected as much as possible, the security of information submitted via the website cannot be guaranteed. Any transmission is done so at the risk to the individual.

Once the information has been received, appropriate technology and operational security has been implemented to safeguard personal information against loss, theft and unauthorised use, access or modification. In the event of any breach which might expose a person to a serious risk, they will be notified promptly.

Links may be provided on the website to other websites that are not operated by Challenger. Use of these links will result in leaving the Challenger website and Challenger is not responsible for the contents of any third-party website.

Disclosure

Like most organisations, Challenger engages service providers to run the IT, payroll and pension processing systems. These companies will only be provided with the information they need to deliver the service they have been engaged for and are prohibited from using that information for any other purpose.

Personal information may also be disclosed to tax, customers and excise authorities; regulators, courts and the Police; central and local government; screening agencies; insurance companies and other professional advisors.

Some of the companies who provide services to Challenger may be located outside the United Kingdom; marketing service providers who are located in the United States, for example. As a result,

personal information may be transferred outside the UK.

Challenger will ensure that those service providers comply with any legal requirements that apply to the transfer of personal information outside the UK, including, where appropriate, requiring the service provider to sign an International Data Transfer Agreement for the transfer of personal information to third countries.

Challenger may also disclose personal information if it is believed that the disclosure is necessary to enforce or apply its terms and conditions or otherwise protect and defend its rights, property or the safety of its customers and other users of the website.

Challenger may disclose and/or transfer personal information in connection with the sale of any part of the business or assets.

Data breach procedure

If Challenger IT systems are beached then a Partner should arrange for the compromised system to be isolated from the network in the first instance. Law enforcement agencies and the ICO should be notified as required, depending on the nature of the breach. Notifications may also need to be made to other agencies such as merchant providers, internet service providers, insurance providers and card services providers.

A Partner should then investigate the incident by gathering a reviewing logs and related information and conducting appropriate forensic analysis of the compromised system. A third-party agency may be used to assist with the investigation. Findings should be made available to law enforcement agencies as required.

The Partner should determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred.

Retention

Challenger will retain the minimum amount of personal information for no longer time than is necessary for the legitimate business purposes described above. Information from website visitor enquiries will be retained for a limited period in order to respond to any queries, provide information and send updates on products and services unless these communications are opted out of. Information may be retained for longer if there are valid legal grounds to do so, for example if required by law or court order, or as needed to defend or pursue legal claims.

Record description	Minimum retention period
CCTV	1 month
Vehicle tracking	1 month
Tachograph records	2 years
Accident book records	3 years

Waste transfer notes	3 years
Customer and supplier records	7 years
Invoice and accounting records	7 years

Changes to this policy

Challenger reserves the right to amend this policy from time to time without notice. Regular review of the website is advised to stay informed of any changes.

Your rights

The following rights are given to a person in relation to personal information:

- the right to be informed, by way of this Policy;
- the right to correct or update any personal information held by Challenger;
- in certain circumstances, to restrict or object to the processing of personal information, or request that personal information is deleted;
- where personal information has been provided voluntarily, or otherwise consented to its use, the right to withdraw consent;
- in certain circumstances, the right to receive a copy of the personal information which has been provided to us, in a structured, commonly used and machine-readable format or to request that the information is transferred to another party (known as 'data portability'); and
- the right to complain to a Data Protection Authority (see further below).

Questions, requests for additional information or requests to exercise the rights of a person may require identification and should be made to a Partner in writing.

If the use of personal information or the response to questions or requests regarding personal information is unsatisfactory, a person has a right to complain to the Information Commissioner.

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

https://ico.org.uk/concerns/

0303 123 1113.