Quadrilect
LTD

# Privacy Statement, Data Processing & Breach Management

Quadrilect LTD

# Data Protection Policy

We, Quadrilect Ltd are required to comply with the provisions of the General Data Protection Regulation GDPR in relation to how we handle any personal data we obtain from you. Any personal information we gather will only be used in the context of your employment with us OR the business we conduct with you. We may also collect Sensitive Personal Data about you, but only with your explicit consent in advance.

We will process the information we obtain from you to enable us to fulfil our contractual obligations and we will only disclose your details to selected third parties where required to deliver the service purchased or a legal requirement, such as Qualification Awarding Organisations, Regulators or Industry bodies.
If you have specified you would like to receive marketing information, we may from time to time email or post to you or your company details of products or courses we believe may be of interest to you. If you no longer require such information or you have provided us with any information that you no longer wish us to use, please contact us on info@quadrilect.co.uk or call us on tel 07483 348224/760.

**Right to be Forgotten**
You have the right to have us correct any inadequacies in the personal details we hold about you, and to object to any direct marketing we carry out using your personal details. You also have the right to ask for a copy of the information we hold in our records. Please contact us at the details below if you require a copy of the personal data we hold about you.

You can at any point make a request to access your information and advise us if you wish for information to be removed. We will respond to this request within 30 days.

You have the right to request removal of this information where it doesn’t breach statutory requirements.
Information on data protection can be found at www.ico.org.uk
You can contact us on
info@quadrilect.co.uk
tel: 07483 348 224/760

**Our digital security**

**Firewall**
The Boundary Firewall of our internal network is “industrial strength” which is closed to all externally instigated traffic from other than white listed IP addresses and uses one time codes, sent via SMS, to control administrator access. Daily firewall reporting is monitored for traffic that has been denied access so as to identify and respond to attempts to break security before a breach is achieved. In addition, we:
a. Action lock-out following failure to enter password, designed to prohibit automatic password hunting.

b. Use industry leading malware protection with real time scanning of emails and file downloads and daily full scanning of system and data files. All with automatic deletion or quarantining of identified threats

**Email and web host**

Our Email service and website are hosted by Network Solutions across a server farm that is divided into a series of separate server pools. Each server pool in the farm is specific to a particular subset of hosting functionality and is protected by its own, industrial strength, firewall. These firewalls are each configured to allow only traffic that is relevant to the particular server pool's purpose. These firewalls are supported by threat detection and prevention software that runs on each of the servers within any particular pool. As with the firewalls, this software is configured to support the security of the particular pool in which it is installed.

Access to the administration and file transfer capabilities of these facilities, Email and website, is secured to privileged users with strong, two factor, authentication.

**Cloud Data Storage**

We use industry leading Cloud service providers to store some of our data. The data concerned is encrypted before transmission to the Cloud, is stored on the Cloud in the encrypted form and remains encrypted for transmission back to our in-house network.

By default, access to files held on the Cloud is limited to the file author. Access may be shared with other specified staff on a need to know basis. All access is protected by two-factor user authentication.

**In-house Network**

Our in-house network is managed on internal servers protected by firewall and two-level authorization.

Cyber Security Certificate

We hold a Cyber Essentials and IASME Certificate and insurance.

**How we use your data**

Training Courses

Data provided to register on a training course is processed to enable us to register you and send out information regarding your attendance at the course.

Name
Job Title
Company
Address
Telephone
Email
Dietary/special access requirement if required

**Where is the data kept?**

This data is kept on our event management database which is hosted on an internal server at a secured location and is not connected to external networks or the internet. Any booking data may also be held on our password / firewall protected network or the two-factor user authentication servers of our Cloud service provider.

**Online registrations**

Reservations submitted via our website involve two pools of the Network Solutions server farm. A web server processes interaction with your browser to collect and validate the information you submit. Thereafter the completed reservation is saved to a SQL database which is running in a separate server pool.

Access to the database is limited to SQL read and write commands and then only from a nominated source (the web server) with two factor authentication. These data are subsequently transferred to, and processed on, Quadrilect's in-house server.

The personal data handling pages of our web site use the "code behind" model. Necessary program code is not downloaded to the browser. Rather, it is kept and executed on the server and not available to the view code feature of the browser. This means that a site visitor can see no clue as to how the data is stored or accessed.

Data transfers between your browser and our website are encrypted in accordance with a valid SSL Certificate issued to Quadrilect Ltd; likewise, any transfers between site facilities and our administrators' systems.

Credit/Debit card Information

Payment is made via Stripe, a secure online payment processing platform. Your web browser is routed directly to the Strip server as you start a payment and only comes back to our web server when the payment transaction is complete. Your credit/debit card details do not pass through our website and are not held on any Quadrilect database.

**Online Accounts**

Data submitted to create and/or manage an online account is captured and stored as previously described for online reservations with the exception that these data are not transferred to a Quadrilect server.

**How long do we hold your data?**

We hold your CPD records on our event management system [off line] and in network folders [firewall and password protected] as a lifelong learning reference. However, if you wish for the data to be removed we are happy to do so on request. We hold financial records for up to 7 years.

**Who do we share this data with?**

A delegate list showing name and company is provided for each course and shared with the course administrator and course trainer/s.
Marketing data on our event management system for public courses

All learners are given a profile as follows:
Delegate – a previous course attendee & Area of interest – eg facilities/health & safety
We are happy to remove this data at any point if you do not wish to be contacted by us. Alternatively, you can choose to have just email communications or just direct mail. Please just contact us and advise on tel: 07483 348 224/760

**Who do we share your data with?**

MS Teams or Zoom Video Conference Platforms for Virtual Training Zone Courses only – you will log in using meeting id we provide via a browser but you do not give any other data other than your name so we can give you access. If you choose to set up an account and download the software directly to your pc then you should check you are comfortable with their privacy and data policy directly.
https://zoom.us/privacy/
https://privacy.microsoft.com/en-gb/privacystatement
Mailing House for Direct Mail Campaigns [return address envelopes for removal requests]. Data protected and destroyed after processed. Hanson Direct Privacy Policy
http://www.hansondirect.co.uk/styled-3/
Dotdigital for e-news campaigns with an unsubscribe option Dotdigital Privacy Policy
https://dotdigital.com/terms/privacy-policy/
Mailchimp for e-news campaigns with an unsubscribe option Mailchimp Privacy Policy
https://mailchimp.com/legal/privacy/
Client - secure document shared with privileged users.
Survey Monkey - Evaluation Survey Survey Monkey Privacy Policy
https://www.surveymonkey.com/mp/legal/privacy-policy/
Connaught – plain text email communications with event information and post course documentation Connaught Privacy Policy requested. https://www.quadrilect.com/event-management_35_3882896022.pdf

For some of our events we request your permission to publish your details in the event delegate booklets.

**Email communications**

All email communications are managed via our Network Solutions Email server. This server runs in another pool of the Network Solutions server farm, a pool whose defences include the scanning incoming mail for known or possible threats and monitoring for, and reacting to, atypical network traffic.

The Email server maintains an in box for each authorised Quadrilect addressee. The messages in each of these inboxes may be seen by the appropriate addressee subject to strong two factor authentication. The majority of messaged are subsequently downloaded to email applications software on one or more of the client systems (desktops, laptops and mobile devices) that are within the scope of the Quadrilect secure network.

All documents with personal data are secured with password protection. A log of portable/mobile devices and content is maintained to manage and destroy data as appropriate.

**Qualifications**

Data provided to register on a Qualification is processed to enable us to register you with the relevant Awarding Organisation and send out information regarding your qualification programme, process assessment and results.

**Where is the data kept?**

As above for training course attendance as outlined in your signed study plans

Learner folders are held on our network which is run on in-house servers with commercial firewall & password protection. These folders contain your application, study plan, assessment submissions and feedback

**How long do we hold this data?**

CPD records are held for lifelong learning as above

Financial data is held for up to 7 years

**Online accounts**

Our on line learning platform for qualifications is Moodle. We set up the learner account and provide user name and password. The accounts are deleted on successful completion of the qualification or registration expires.

Plagiarism Software

All assessments are processed through a plagiarism software tool, Plagscan [secure access for privileged users]. This will generate a report on the assessment to ensure the work is properly referenced and has not been copied from another source without the correct acknowledgements. Once an assessment has been processed and the report generated the information is deleted.

## Conferences, Dinners and Events

### What data do we hold?

For the purpose of processing your registration we collect the following data.
Name
Job Title / Profession
Company
Address
Telephone
Email

### Where do we hold it?

This data is kept on our event management database which is hosted on an internal server at a secured office location and is not connected to external networks or the internet. Any booking data may also be held on our password / firewall protected network or the two-factor user authentication servers of our Cloud service provider.

### How long do we hold it?

We hold your CPD records on this system as a lifelong learning reference. However if you wish for the data to be removed we are happy to do so on request. We hold financial records for up to 7 years.

### Who do we share it with?

Zoom Video Conference Platform for online events – For large online events you will be asked to register directly with zoom but they will not sell or re-use your data. Please see their privacy policy below
https://zoom.us/privacy/
MS Teams – for purpose of issuing invitations and hosting virtual training

### Who is responsible for personal data in Microsoft Teams?

To the extent Microsoft Teams processes personal data in connection with Microsoft's legitimate business operations, Microsoft will be an independent data controller for such use and will be responsible for complying with all applicable laws and controller obligations. Microsoft Teams Privacy - Microsoft Teams |
Microsoft Docs
docs.microsoft.com/en-us/MicrosoftTeams/teams-privacy
HopIN – for purpose of issuing invitations and hosting virtual training
Hopin's purpose in establishing this privacy policy is to give you information about how Hopin collects and processes your personal data through your use of the Hopin Services, including any data you may provide through the Hopin platform. Hopin Privacy Policy
hopin.com/legal/privacy
Mailing House for Direct Mail Campaigns [return address envelopes for removal requests]. Data

protected and destroyed after processed. Hanson Direct Privacy Policy
http://www.hansondirect.co.uk/styled-3/
Dotdigital for e-news campaigns with an unsubscribe option Dotdigital Privacy Policy
https://dotdigital.com/terms/privacy-policy/
Mailchimp for e-news campaigns with an unsubscribe option Mailchimp Privacy Policy
https://mailchimp.com/legal/privacy/
Client - secure document shared with privileged users.
Survey Monkey - Evaluation Survey Survey Monkey Privacy Policy
https://www.surveymonkey.com/mp/legal/privacy-policy/
Connaught – plain text email communications with event information and post course documentation.
https://www.quadrilect.com/event-management_35_3882896022.pdf
For some of our events we request your permission to publish your details in the event delegate booklets.

**Other**

**Email communications**
All email communications are managed via our Network Solutions Email server. This server runs in another pool of the Network Solutions server farm, a pool whose defences include the scanning incoming mail for known or possible threats and monitoring for, and reacting to, atypical network traffic.
The Email server maintains an in box for each authorised Quadrilect addressee. The messages in each of these inboxes may be seen by the appropriate addressee subject to strong two factor authentication. The majority of messaged are subsequently downloaded to email applications software on one or more of the client systems (desktops, laptops and mobile devices) that are within the scope of the Quadrilect secure network.
All documents with personal data are secured with password protection. A log of portable/mobile devices and content is maintained to manage and destroy data as appropriate.

**Supplier Data**
We use Sage Accounts to manage our supplier accounts and hold the following information.
Company name, address and bank details. This information is held so we can process supplier invoices for services received.
Sage Accounts is held on our secure internal network and only accessed by privileged users with password protection.

**Data Breach Management**
Daily firewall reporting monitored and quarterly periodic testing of system access. If a breach is identified we will alert all customers and suppliers via email and put a notice on our website outlining the form of the breach and data exposed. All security passwords will be updated and system access points restored with new IP addresses where required.

Customers will be asked to change their account passwords.
Note no credit/debit card data is stored as we use a payments processing platform.

**Changes to our data processing**
We will update this policy if any change to our data processing occurs and this will be published on our website. A link will be provided to this policy with the confirmation of all training & qualification registrations. If there is a fundamental change of the type of data we are processing and the use of data we will send an email communication to all suppliers and customers updating them on our processes with a link to the updated policy.

**Data Destruction**
Any request for data to be deleted where it doesn't breach statutory requirements will be processed within 48 hours. Notification will be sent confirming the data destruction.
System hardware will be disposed of through a certified company and certificates of destruction will be held for audit purposes.
Hard copy data with personal identifiers will be destroyed by a certified shredding company and certificates of destruction will be held for audit purposes.
Hard copy data stored with a secure storage facility is annually reviewed and an archive document is updated recording content and date of destruction.