GDPR Policy

Contents

GDPR Policy

AE Exchange Ltd is committed to protecting both the privacy of signed up users of the AE Exchange website, www.aeexchange.com, and any of its applications (the “Website”) and the security of any information which its users provide. This privacy policy discloses the ways we collect and manage your data and our compliance with GDPR.

This Policy shall become effective on 1st April 2018 and applies between

- Us, AE Exchange.com of Unit 101, China house, 395 Edgware Road, London, NW2 6LN, (hereinafter referred to as the “Data Processor”, “we”, “our”, “us”); and

- You, the signed up user of our Website and any associated Applications (hereinafter referred to as “you”, “user”).

We agree to store, process and/or e-file the Data you voluntarily provide to us
(a) only as voluntarily and expressly instructed by you within the provisions of the Website's Terms of Service
(b) for the sole purpose of fulfilling the services as offered on our Website, and
(c) in accordance with Applicable Law.

This Policy shall be governed by and construed in accordance with English law and the exclusive jurisdiction of the English Courts.

1. What is “Data”?

The GDPR applies to personal data (hereinafter referred to as “Data”) meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data and/or online identifier.
For examples of the kind of Data we may collect, refer to **Appendix A**.

2. Why do we collect Data?

Our Website offers the facilities for you to e-file your Data to HMRC, Companies House and Pension Companies and download your DPS notices from HMRC. By its very nature provision of these services necessitates the collection of personal Data from our users.

3. What Data is Collected and How is it Used?

Three types of Data may be collected from you.

3.1 Data Collected automatically

We use Data collected automatically to help us to, among other things, administer the Website, help diagnose problems with our servers, track users' web page movements, and to keep the Website up to date and interesting for you as well as comply with our legal obligations.

3.2 Data you provide to us for Sign Up/Sign In

We require personally identifying Data when you sign up with us in order to create a secured sign in procedure for you to access your account and the data it contains. Once you sign up with our Website and sign in to our services, you are not anonymous to us.
We may on occasion use the email address and other contact details you provided to us on sign up to contact you regarding service orientated issues, for example regarding invoicing, new services, how the services can be used

effectively, announcements and/or inviting customer feedback on the services we provide. We may also use this identifying Data for policing of our users' accounts.
We undertake not to send you undue or uninvited marketing email material.

3.3 Data you provide to us for Processing

This data is required in order to provide you with the e-filing and/or downloading services and/or other services you have signed up to our Website and/or associated Applications for.
We reformat the necessary Data you provide and transmit it on your command to your chosen destination i.e. HMRC, Companies House, Pension companies and/or any third parties you may have chosen, e.g. bank or credit card companies. In addition, you may make use of our Website to store, view, download and/or to print out the data and documents relating to the e-filing and downloading.

Data collected may include data about yourself and/or your employers, employees and/or your clients and their employees. Data is collected by spreadsheets uploaded by you to our Website, or by the keying in of Data directly into our Websites, or through data interchange technologies e.g. API or SFTP.

Details and an example of what Data is collected is set out in the **Appendix A** of this Policy. This Appendix will be regularly reviewed and updated to ensure that the contents are accurate and up-to-date.

Privacy by design: We have undertaken to design our Website in such a way to minimise the collection and use of Data. We will advise prior to collection whether the provision of the requested Data is compulsory or whether the information may be provided on a voluntary basis.

Consent: You must seek and gain the consent of your employer, your employees, clients and/or their employees BEFORE passing any of their data to our Website or extracting any of their data from our Website. You must also inform all those who consent to have their Data stored by us, exactly what data will be stored, and for what purposes it is stored. You agree to take full responsibilities in ensuring full consent are sought from all the stakeholders concerned. Our Website is open to all users to use and if you continue to sign up and create an account and use our Website we can only assume that you have gained prior consent from all the parties mentioned in this paragraph.

Although we may on occasion scan the database when required for administrative and invoicing purposes, we do not monitor, edit or review whether the data provided by you is correct or complete. We maintain a strict policy not to access any user's account uninvited and will not modify any data stored in our system. However, to facilitate the convenience of tax codes and student loan update our system may conduct auto-update of this information whenever HMRC provide such update data. You alone are responsible for the accuracy and completeness of your records and updating the data as required. We will only validate your data through automatic processes to check that it conforms to the formatting schema required for successful submission to HMRC, Companies House and/or Pension companies.

Employee Users

If you are an employee of a company using our Website and you do not wish to receive emailed or mobile payslips or have access to an online account to view your payslips online you have every right ask your employer not to enter your email address or mobile phone number into our system. If you already have an online account you can close that account with us forever by clicking on the Close Account option after logging in to your account and following the instructions. Alternatively, you have every right to ask your employer to remove your email address or mobile number and/or disable your employee account.

If you are an employee of a company using our Website you have every right to ask for your Employer to help to delete from our system any data relating to you which is not legally required to be kept in our system. To do this please inform your employer that you do not want to have your non-statutory required data held in our system and ask them to remove your data from our system. We do not entertain any requests for deletion of employee data ourselves, you must ask your employer to delete the data. We do not and will not access to any user's account to modify any data stored in our system. The only person that can help you to delete what is legally allowed to be deleted data is your employer. If you object to this arrangement on how your data can be deleted you should discuss it with your employer on how to take the matter further.

If you are an employee of a company using our Website and you do have an online account with us to view your payslips online you should be aware that your access to that account will cease if your company ceases operation, closes their account with us, or allows their account with us to lapse. Therefore, to ensure you always have a copy of your payslips you should always download and save your payslips from your online account to your own system/device in case your access to your online account ceases.

3.4 Cookies

Cookies are small text files that are placed on your computer, smartphone or other device when you access the internet which enable users to navigate around the Website and (where appropriate) let us tailor the content to fit the needs of our users.
None of the cookies we use collect your Personal Data and they can’t be used to identify you. The length of time a cookie stays on your device depends on its type.

We use three types of Cookie categories
A. Strictly necessary
B. Performance
C. Functionality

A. Strictly necessary
'Strictly necessary' cookies let you move around the Website and use features like secure areas and in some cases online billing. These cookies don't gather any information about you that could be used for marketing or remembering where you've been on the Internet.

We use these to:
- Remember things like information you've entered on forms when you navigate to different pages in a single web browser session
- Identify you as being logged in
- Make sure you connect to the right service on our Website when we make any changes to the way the Website works

We do not use these to:
- Gather information that could be used to advertise products or services to you
- Remember your preferences or log in details beyond your current visit

Accepting these cookies is a condition of using our Website, so if you prevent these cookies we cannot guarantee your security or predict how our Website will perform during your visit.

B. Performance

'Performance' cookies collect information about how you use our Website, for example, which pages you visit, and if you experience any errors. These cookies don't collect any information that could identify you – all the information collected is anonymous and is only used to help us improve how our Website works and understand what interests our users.

We use these to:

Provide statistics on how our Website is used

C. Functionality

'Functionality' cookies are used to provide services or to remember settings to improve your visit.

We use these to:

- Remember settings you've applied
- Provide proactive live chat sessions to offer you support
- Show you when you're logged in to the Website
- Share information with partners to provide a service on our Website. The information shared is only to be used to provide the service or function and not for any other purpose

We do not use these to:

- Target you with adverts on other websites

Some of these cookies are managed for us by third parties – where this is the case we don't allow the third party to use the cookies for any purpose other than those listed above.

You can control whether or not these cookies are used, but preventing them may mean we can't offer you some services and will reduce the support we can offer you. It's also possible that preventing these cookie stops us remembering that you didn't want a specific service.

In order to use our Website you must have the cookies enabled on the settings of your device. We use cookies to ensure that we give you the best experience on our Website. If you sign up/sign in to our Website with Cookies enabled in your device setting we will assume that you are happy to receive all cookies from our Website. However, you can change your cookie settings at any time.

4. Our Duty of Care and Use Restrictions under GDPR

Our provisions to promote accountability and governance: As a Data Processor we are fully committed to our duty to safeguard and secure your data. We will treat your data with as much care as if it were our own. As part of this we maintain UKAS ISO 27001 certification. Further details relating to our comprehensive Information Security Policies can be found in **Appendix B**.

4.1 Data processing rights and obligations

We shall process your Data in accordance with the GDPRs, and will not make any use of your Data or allow any use of your Data except as strictly necessary for the purpose of the services offered on our Website and in particular will not use any of the Data for our own or any other commercial purposes.

4.2 Security and Confidentiality of the Data

We shall hold your Data in the strictest confidence and shall not disclose or allow access to the Data or any part of the Data without your prior consent.
We will not disclose the Data to anyone except your intended recipients or if we are required to do so by law or are ordered to do so by a Court.
We shall restrict access to your Data by our own Personnel - access will be limited to only those Personnel that are required to have access to the Data for the purpose of providing the services offered.

4.3 Our Personnel

We shall ensure that our Personnel:

- are reliable and fit and proper persons to have access to your Data
- are informed of the confidential nature of the Data and are bound by contractual or statutory confidentiality obligations in relation to the Data; and
- have received appropriate, regular and recent training and guidance on data protection and security.

4.4 Our Technical and Operational safeguarding measures

We shall:

- implement and maintain appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing, destruction, loss, alteration, damage to or disclosure of, or access to, your Data.
- ensure that the technical and organisational measures implemented are appropriate to the risks presented by its processing of the Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and the harm that might result from the accidental, unauthorised or unlawful processing, destruction, loss, alteration, damage to or disclosure of, or access to, the Data; and
- regularly review and update the technical and organisational measures implemented.
- maintain a fully resourced and funded Data Protection Officer

4.5 Data Protection Officer

Our Data Protection Officer's minimum tasks will be:

- To inform and advise our personnel about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train personnel and conduct internal audits.
- To be the first point of contact for individuals whose data is processed (employers, employees, clients, etc) and report directly to the board of Directors.

4.6 International transfers of Data

We shall not transfer your Data outside the European Economic Area (EEA), the European Union (EU) or the UK without your prior written consent.

4.7 Sub-contracting

We shall not, without your written consent, allow any third party sub-contractor to process your Data. In the event that you do provide written consent to processing of the Data by a third party, we shall to the best of our abilities ensure that the third party has implemented and maintained technical and organisational means to prevent unauthorised or unlawful processing of or accidental loss of or destruction of the Data.

4.8 Risk Assessments

We will conduct regular data privacy impact assessments (DPIAs) to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of electronic, paper, and other records containing Data and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting such risks.

4.9 Data breaches - Notification

We shall notify you without undue delay and within 72 hours if we become aware of any actual breach or reasonable grounds for suspicion of a Data breach including without limitation any actual or suspected personal data breach affecting the Data.
We shall include in our notification:
- a description of the nature of the breach
- the details of our contact who can provide further information about the breach;
-a description of the likely consequences of the breach,
-a description of the initial remedial measures taken or proposed to be taken to address the breach,

4.10 Record keeping

We shall keep records of the processing of the Data and all information necessary to demonstrate our compliance with the GDPRs. We shall on reasonable notice make available on request all information necessary to demonstrate compliance with GDPR obligations.

4.11 Links to Third Party Sites

Our Website may provide links for you to access third party sites only as a convenience and the inclusion of any link does not imply our endorsement of that particular website. You are responsible for viewing and abiding by the respective privacy statements and terms of use posted on any linked sites. We accept no liability for the privacy practices or content of websites that may be linked to from our Website. This privacy statement applies solely to information collected by our Website.

4.12 Notification of Changes

We may update this GDPR Policy to reflect changes to data protection practices. If any material changes are made a prominent change notification will be displayed on our Website prior to the change becoming effective. You should review this page for the latest information on our privacy practices each time you visit our Website.

4.13 Communications

If we receive any complaint, notice or communication which relates directly to the processing of the Data or to either our or your compliance with the Data Protection Laws, we shall immediately notify you and where necessary provide you with assistance in relation to any such complaint, notice or communication.

4.14 Transaction Monitoring

You understand and accept that the system needs to be in line with HMRC's Transaction Monitoring (TxM) implementation policy and has incorporated these policies in the Website.
Transaction Monitoring (TxM) is a key security approach adopted in the UK and globally. HMRC's approach is in line with National Cyber Security Centre (NCSC) and Cabinet Office recommended guidance and industry good practice. HMRC monitors transactions to protect taxpayers from infringement of their data by criminals or fraudsters. Without the protection offered by TxM, personal data could be compromised, leading to fraud against taxpayers or the UK Exchequer. We are helping HMRC to protect users' confidential data by sending them particular types of user audit data which they will record. We use HMRC APIs with HTTP headers to pass this audit data to HMRC. These headers can influence the processing of the API call, or support HMRC's prosecutions for tax or duty fraud.

5. Your Rights Under GDPR

5.1 Right to Access the Personal Information We Hold about You

In accordance with Applicable Law, you have the right to access the Data we hold about you. You can do this at any time by signing in to your account on our Website and viewing the data in your account or requesting that your company system administrator discloses the material facts to you. Please note that if your account has lapsed due to inactivity we may, depending on the Applicable Law, be entitled to charge a reasonable fee to cover some of our administration costs incurred by re-instating your access to a lapsed account. For security reasons we may also ask you to further verify your identity and to provide more details about your request.

5.2 Right to Rectify Your Data

It is your responsibility to ensure that you submit true, accurate and complete information to us. By signing in to your account you have the facilities to review all data which you upload to our Website and to make changes to any data prior to it being e-filed. We do not and will not modify any user's data on their behalf. Any modification of data must be carried out by the System Administrator or any Additional Users appointed by the System Administrator at their sole discretion. Please be aware that after Data has been e-filed to HMRC or Companies House it is not possible to amend that Data.

5.3 Right to Data Portability

You have the right to download your Data from our Website at any time. To do so sign in to your account and visit the Reports section to download your data. Data will be made available electronically in the commonly used PDF and/or CSV formats.

5.4 Right to Restrict Processing

When you pass us your data through the data interchange channel or by uploading or entering your data directly to our Website, your data will only be processed in accordance to your data processing set up instructions in the Chart of Setup section or the default setting. Likewise, data will only be downloaded from HMRC's DPS service with your permission indicated by you entering your HMRC credentials into your account on our Website. To stop any further downloading you should delete your HMRC credentials from our Website.

5.5 Right to Erasure/Closure of your Account/'Right to be Forgotten'

At the moment we are legally obliged to retain your e-filed Data for a minimum period of six years as required and stipulated by HMRC's policy for tax record purposes. It cannot be deleted during this period. After the minimum period the data can be deleted from our system on request.
HMRC are yet to publish their detailed policy on data deletion. As soon as they do we will update our policy and practices accordingly to comply.
You have the right to close your account with us at any time. If you do this you will no longer be able to access your data, and all/any other user accounts associated with your account, including additional users, client users, employees etc. will be closed and those users will not be able to access their data.

5.6 Right to Object

If you have any questions of concerns about this GDPR Policy and/or our practices regarding Data Protection , or would like to exercise your rights in relation to your Data, please contact our Data Protection Officer, write to: The Data Protection Officer, AE Exchange Ltd, Unit 101, China House, 395 Edgware Road, London, NW2 6LN. To ensure your correspondence reaches us you undertake to send it to us by recorded delivery post.

If you have a complaint or concern about how we are processing your Data we will endeavour to address such concern(s). However, if you would like to direct your complaint/concerns to a Data Protection Authority, the contact details for your local Data Protection Authority are as follows: https://ico.org.uk/global/contact-us/ (https://ico.org.uk/global/contact-us/).

Appendix A

What Data Do We Collect?

Further details of the Data being processed and the nature and the purpose of the processing.

A1) Data Collected Automatically

Whenever you visit or interact with the Website, we may use a variety of technologies that automatically or passively collect information about how the Website is accessed and used. The Personal Data collected is used to improve the appropriateness of the services provided on the Website.

Data collected automatically may include:

- IP address or other unique identifier for the computer, mobile phone, tablet or other device you use to access the Website
- Device type
- Demographics
- Location
- Language
- Type of browser software and operating system you are using
- Page(s) served, the time, and the preceding page views
- Event type (pages viewed/documents downloaded)
- Event date/time
- Page URL
- Downloaded item URL
- Email address
- Organisation type (access permissions)
- Organisation name
- Telephone number
- Date of form submission

A2) Data You Provide to Us for Sign up/Sign in

We will collect personally identifying information when you sign up in order to create a secured sign in to account function. We will ask for your full name, address, e-mail address, and other information we may decide upon from time to time.

A3) Data You Provide to Us for Processing

We provide Human Resource services, accounting, payroll, CIS and pension calculation services and e-filing services to HMRC and Pension Companies, and downloading services from HMRC.

Providing these services necessitates the collection of detailed data relating to Payroll, CIS and pensions.

Below is an example of the Data currently required by HMRC for a Full Payment Submission (FPS) returns. Other

returns require similarly detailed quantities of Data.

(Note that this may change in line with HMRC requirements).

Employer Details – including:

- Employer Name
- PAYE Reference (Tax Office Number / Tax Office Reference)
- Accounts Office Reference
- SA UTR
- Company Tax Reference (Company UTR)
- Employer Address
- Employer Bacs Service User Number (SUN)

Employee Details – including:

- Week No / Month No
- Pay Frequency
- Payment Date
- Payment Method
- Number of earnings periods covered by this payment
- Title
- Forename
- Surname
- Employee Address
- Date of Birth (DD/MM/YYYY)
- Gender (male / female)
- NI Number
- Works Number / Payroll ID
- Payroll ID changed indication
- Old Payroll ID
- Passport No
- Employee Start Date
- Start Declaration
- Student Loan Start Indicator
- Occupational Pension for recently Bereaved Spouse or Partner ?

- Annual amount of Occupational pension
- Employee Leaving Date
- Hours Worked (A,B,C,D,E)
- Taxcode
- Non-Cumulative indicator
- Tax Regime
- Tax Week of Appointment of Director
- Irregular Employment Payment Pattern Indicator
- Taxable Pay in this pay period (Box 58)
- Occupational Pension or Annuity Payment Indicator
- Trivial Commutation Payment Type(s)
- Trivial Commutation Payment Amount(s)
- Benefits value taxed via payroll in this pay period (Box 60)
- Payment value not subject to Tax or NIC (Box 58A)
- Pay after Statutory deductions (Box 59)
- Payment to Non-Individual Indicator
- Payment after Leaving Indicator
- Aggregated earnings Indicator • Taxable Pay TD in this employment (Box 41A)
- Benefits value taxed via payroll YTD in this employment (Box 149)
- Tax deducted or refunded in this pay period (Box 68)
- Student Loan repayment in this pay period
- Employee Pension Contributions under net pay arrangements in this pay period
- Employee Pension Contributions not under net pay arrangements in this pay period
- On Strike Indicator
- Unpaid Absence Indicator
- Items subject to Class 1 NIC but not taxed under PAYE excluding Pension in this pay period
- Deductions value from Net pay in this pay period (Box 58B)
- Total Tax TD in this employment (Box 41B)
- Total Student Loan repayment recovered YTD in this employment
- Employee Pension Contributions YTD under net pay arrangements in this employment (Box 150)
- Employee Pension Contributions YTD not under net pay arrangements in this employment (Box 151)
- NIC Table Letter 1 in this pay period
- Gross Earnings for NICs in this pay period 1
- Gross Earnings for NICs YTD 1
- At LEL 1 YTD

- LEL to PT 1 YTD
- PT to UEL 1 YTD
- Total of Employer NI Contributions in this pay period 1
- Total of Employer NI Contributions 1 YTD
- Employee NI Contributions in this pay period 1
- Employee NI Contributions 1 YTD
- NIC Table Letter 2 in this pay period
- Gross Earnings for NICs in this pay period 2
- Gross Earnings for NICs YTD 2
- At LEL 2 YTD
- LEL to PT 2 YTD
- PT to UEL 2 YTD
- Total of Employer NI Contributions in this pay period 2
- Total of Employer NI Contributions 2 YTD
- Employee NI Contributions in this pay period 2
- Employee NI Contributions 2 YTD
- NIC Table Letter 3 in this pay period
- Gross Earnings for NICs in this pay period 3
- Gross Earnings for NICs YTD 3
- At LEL 3 YTD
- LEL to PT 3 YTD
- PT to UEL 3 YTD
- Total of Employer NI Contributions in this pay period 3
- Total of Employer NI Contributions 3 YTD
- Employee NI Contributions in this pay period 3
- Employee NI Contributions 3 YTD
- NIC Table Letter 4 in this pay period
- Gross Earnings for NICs in this pay period 4
- Gross Earnings for NICs YTD 4
- At LEL 4 YTD
- LEL to PT 4 YTD
- PT to UEL 4 YTD
- Total of Employer NI Contributions in this pay period 4
- Total of Employer NI Contributions 4 YTD
- Employee NI Contributions in this pay period 4

- Employee NI Contributions 4 YTD
- Director's NIC method of calculation
- Employer Name in Bank Account
- Employer Bank Sort Code
- Employer Bank Account Number
- Employee Name in Bank Account
- Employee Bank Sort Code
- Employee Bank Account Number
- User Reference (Roll Number)
- Bacs HASH Code
- Random String
- Employee Seconded to work in UK - Type (A, B or C) ?
- If Employee, is a European Economic Area or Commonwealth citizen ?
- If Employee is under EPM 6 (modified) scheme ?
- Late PAYE Reporting reason (A,B,C,D,F,G,H)
- SMP YTD
- SPP YTD
- SAP YTD
- ShPP YTD
- Partner NINO
- Partner Initials
- Partner First Forename
- Partner Second Forename
- Partner Surname
- P45 Part 1 Taxable Pay TD
- P45 Part 1 Tax TD
- P45 Part 1 Deceased Indicator
- P60 Previous Employment Taxable Pay TD
- P60 Previous Employment Tax TD
- P60 Week 53 Indicator
- Email
- Flexibly accessing Pension Rights
- Pension Death Benefit
- Serious Ill Health Lump Sum Indicator
- Flexible drawdown Taxable Payment

- Flexible drawdown Non-taxable Payment
- Car Make(s)
- CO2 Emissions for car(s)
- Car Fuel Type(s)
- Car Identifier(s) (Car Registration No)
- Amendment Indicator(s)
- Calculated Price(s)
- Dates Car was available From (DD/MM/YYYY)
- Cash equivalent of Car(s)
- Dates Car was available To (DD/MM/YYYY)
- Dates on which Free fuel was provided (DD/MM/YYYY)
- Cash equivalent of Fuel
- Dates on which Free fuel was withdrawn (DD/MM/YYYY)

Appendix B

Our Information Security Policy

As a Data Processor we have a responsibility for promoting good practice in information security across our organisation and for monitoring the effectiveness of information security.

Our information security policy is summarised below:
We require that:
- that any confidential information shall when not in use be placed in a secure location and the imposition of a 'clear desk' policy; and
- personnel to log-off of systems when leaving a terminal/workstation unattended.

B1) Personnel

We shall:
- ensure that Personnel who have access to the Data are vetted prior to commencing work to ensure that they are reliable and fit and proper persons to have access to the Data;
- adequately train its Personnel on data protection and security;

- ensure that Personnel understand their obligations to keep the Data secure and confidential;
- ensure that Personnel have committed themselves to binding confidentiality obligations;
- ensure segregation of duties for critical and sensitive roles and reduce reliance on key individuals; and,
- operate a joiner, movers and leavers process to grant, amend or revoke access privileges promptly for users of systems and applications processing Data.

B2) Business continuity and incident management

We shall:

- define procedures for dealing with incidents including without limitation investigation, planning of remedial action, resolution, communications, supervising activity and documenting actions taken;
- have business continuity strategies and processes/ disaster recovery plans including (without limitation) the ability to restore the availability of and access to the Data in a timely manner in the event of a physical or technical incident; and
- regularly back-up copies of the Data stored securely and separately from the live files.

B3) Virus and malware protection

We shall:

- have in place industry recognised virus and malware protection software and techniques to prevent infection by viruses and malware
- maintain the use of automatic update mechanisms for anti-virus software
- Regularly review the software and data content of systems supporting critical business processes and the presence of any unapproved files or unauthorised amendments shall be formally investigated.

B4) Security monitoring and audit

We shall maintain our UKAS ISO27001 certification and:

- have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in place for ensuring the security of the processing of the Data;
- have the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
- shall regularly carry out monitoring, testing and audits of the measures in place to keep the Data secure and confidential and make improvements based on the recommendations coming out of such monitoring, testing and audits.

B5) Access controls

We shall ensure that we have in place procedures that control access to files, documents and systems containing the Data. We shall ensure that the access control arrangements:

- cover access by all Personnel including without limitation, business users, individuals running the system and specialist IT staff, such as technical support staff;
- include password controlled access to systems
- restrict access to the Data in line with access control policies;

B6) Communication, transmission and storage of Data

We shall:

- use encryption as appropriate when the Data is in transit and at rest;
- not use, reproduce or store any of the Data on an externally accessible computer or electronic information retrieval system; and
- implement controls to prevent the Data being sent to or access by unauthorised parties.

B7) Physical and environmental security

We shall control access to facilities where Data is processed and have in place adequate precautions against unauthorised access by:

- fitting intruder alarms and locks activated by fingerprint/facial recognition;
- recording the arrival / departure of visitors and supervising them at all times;
- providing CCTV surveillance.

B8) Destruction and deletion of data

We shall as necessary implement appropriate measures to securely destroy and permanently delete files and documents containing the Data.