How do you ensure that client data is protected and your systems are secure?

At Zurich we welcome the uniformity that the General Data Protection Regulation (GDPR) is designed to bring to the European data protection landscape. The differences in the data protection laws of the EU Member States under the previous regime were significant, even though they were all based on the same Directive. The uniformity intended by GDPR should facilitate the ease of doing business in or with the EU, while ensuring a high level of data protection for individuals.

We take our data protection obligations extremely seriously and the security of our customer data is very important to us. We rely on personal data to accurately and effectively assess risk and provide customers with cover and investment opportunities that meet their needs. We are ensuring that our alignment on regulatory interpretation enables continuing delivery of GDPR compliance, specifically taking care of the individual’s rights and freedoms, transparency of their data processing and, where applicable, carrying out Privacy Impact Assessments. This activity is managed by a dedicated Data Protection team at Zurich UK that includes our appointed and mandated Data Protection Officer (DPO) Marnee Baker.

All Zurich employees receive periodic training with respect to data protection and privacy. Specific training is provided to individuals working in areas that interact with high volumes of personal data (including handling data subject requests) and sensitive personal data. Zurich’s relevant policies and procedures include authority and access limitations.

Platform operator SIML is GDPR compliant. We can action all data subject requests and are compliant in all material areas. We have a programme of activity that is undertaking work on a number of our older systems to ensure that we can routinely remove data at the end of our retention period.

Fraud prevention is a key activity at Zurich, including safeguarding against identity fraud. We have a suite of internal training and support materials that staff absorb on a repeated basis, to mitigate against such fraudulent activity. For security reasons, we do not externally divulge details of infiltration attempts, but promptly act upon any instances to further bolster our controls. Indeed, our framework of controls that ensure we adhere to our regulatory requirements encompass all financial crime, including anti-money laundering, tax evasion, fraud, anti-bribery and corruption. These controls are rigorously tested and monitored regularly to ensure they remain fit for purpose.

Not least, we have just publicly announced our industry-leading Data Commitment in the UK, where we express an unwavering commitment to our customers to:

• keep their data safe
• never sell their personal data
• not share their personal data without being transparent about it
• put their data to work so we can better protect them, and so they can get the most out of life.

With regard to Zurich’s Wealth Platform, this transparency initiative should reassure advisers and their clients that Zurich takes its data protection responsibilities seriously and will continuously focus on safeguarding clients’ rights in the spirit of relevant legislation and regulation.

How robust is your Information Security Management System?

Zurich has a global information security framework incorporating standards owned by the Global Information Security function and approved by the Group Board.

This framework includes policies and processes regarding data and information security and the usage of IT equipment and assets. These are supplemented as required by specific local policies, for example: use of email, social media, removable media, physical security, etc.

Zurich also has dedicated Architecture, IT Governance, and Supplier Assurance functions, each with formal processes, checkpoints and approval processes. These provide robust management, audit and oversight of these related functions.

Zurich is a Financial Services company and not a supplier of IT Services; therefore we have not sought to obtain ISO (International Standards Organisation) certification. However, we do comply with best practice data information security policies, and measures are in place which are aligned with the requirements of the ISO 27001 standards as set out in the Zurich IT Risk Standards & Consolidated IT Controls Catalogue. Zurich’s third-party suppliers are contractually obliged to provide assurances to Zurich that as IT service providers they are complying with/attaining certifications for standards such as ISO 27001, ISAE 3402, AA01/06.

In addition to the above we also monitor both industry and general best practice and keep abreast of requirements (such as Cyber Essentials).
What controls and risk assessments do you place on third parties?
As mentioned above, third parties are obliged to comply with Zurich’s data protection and information security controls and requirements.

All third parties (vendors, suppliers, etc.) provide services under contract and Zurich has a robust and comprehensive supplier assurance and governance framework to ensure third parties and business partners meet our minimum standards in all areas – including security and data protection. It is also a requirement for Zurich’s third-party/strategic suppliers to perform vetting of all their staff who are engaged on the Zurich account.

How are your network and servers protected against external threats and attacks?
Zurich has a layered approach to security that, for externally facing systems, incorporates but is not limited to: firewalls, IPS, DDoS protection, DLP, load balancing, etc. We also perform regular perimeter and network vulnerability scanning and penetration testing.

At network level this includes elements such as anti-virus, IDS, APT detection as well as device hardening to ensure access to components such as routers and switches is restricted to authorised users only on a ‘least privileged’ basis.

Prioritisation of application/system protection is focused on Classification of data held in or processed by the system/application and Business Criticality. This prioritisation informs the ‘Assurance Level’ for systems and, further to this, the application of security standards, tools and requirements.

Security of workstations and mobile devices is centrally managed and implements controls around the use of portable media. Controls such as AV, DAC, DLP and device encryption apply at this level.

With regard to mobile devices (smartphones), an enterprise Mobile Device Management solution is in place to enable secure use of approved devices.

How do you respond to a cyber security incident?
Zurich has significant and robust measures in place to maintain cyber security. We have a dedicated Cyber Security team that is part of our wider Group Information Security team and standards that align to ISO 27001. Pre-emptively, Zurich employs mandatory security testing independently run by Veracode, and also Manual Penetration Testing for all systems at least once per year and upon all significant change. This is in line with our Group Information Security function’s security standards.

We would consider a data security breach to be an event impacting the Confidentiality, Integrity or Availability of data (there are varying levels of severity). At Zurich we use a formal incident reporting, management and resolution process with a defined set of response levels and escalation paths depending on the severity of the event.

All systems run under an agreed operational response framework which is reviewed monthly within our dedicated service management organisation; this covers security breaches, system incidents and also disaster recovery (DR) scenarios.

Depending on the severity of the incident or DR situation, the organisation has different levels of response teams who will be invoked accordingly. The teams are responsible for the coordination and management of the incident through to resolution.

Note that internally, we have mandatory Information Security (including Cyber Security) training for all staff that must be repeated annually as a minimum.

What data recovery, business continuity and disaster recovery plans do you have?

Data recovery
As part of our information security framework, the conservation of data is a key objective.

Data is stored in the UK London Data Centre, a Tier 3 certified site. Traditional data centre controls are in place e.g. physical, environmental, DR and BC controls. The data centre complies with Zurich IT Risk Standards.

Zurich has multiple systems across the UK and each has a back-up strategy. Back-ups of essential information (e.g. business information, systems information and application information) and software are performed frequently enough to meet business requirements in accordance with Zurich’s defined back-up/archive schedule that reflects the security classification and time criticality of the information and software being backed up.

IT disaster recovery tests of critical systems are conducted on a quarterly basis. This is to prove the RTO (recovery time objective)/RPO (recovery point objective) requirements can be achieved.

Business continuity/disaster recovery
We have a UK Disaster Recovery and Business Continuity team that routinely runs exercises to ensure we can recover from service interruptions if they occur.

Within Zurich, the importance of Business Continuity Management (BCM) is recognised and reflected in the Zurich Risk Policy. BCM offers a way to manage some of the operational risks that arise from people, processes, systems and external events. Zurich has a robust BCM framework in place; this is managed by a team of business continuity professionals including Business Continuity Managers. The BCM framework is in line with Group Risk policy and the British Standard for Business Continuity ISO 22301.

Zurich’s business continuity planning incorporates five major impact categories: loss of building, denial of access to buildings, loss of IT and telephony, loss of key staff (including pandemic) and loss of key suppliers. Business continuity plans are reviewed at least quarterly and exercised at least annually. We maintain a comprehensive set of BC plans covering all critical aspects of our operations – and all aspects of TCF are considered in these plans to specifically ensure Zurich delivers fair outcomes, even in the event of a serious incident causing business disruption.

Zurich is dedicated to yearly testing and exercising of its business continuity capability to ensure we remain resilient.

The BCM process is reviewed regularly to ensure that changes in business requirements are reflected in the strategies and incorporated into BC plans.
Are staff user privileges and data access rights controlled?
Zurich Identity and Access Management policy ensures access is granted in line with role and responsibility on the basis of least privilege. Access is managed centrally via our Identity and Access Management System.

All users have unique IDs and passwords, which are never shared. Both preventive and detective process and technical controls are in place to enforce separation of duties.

Well-defined processes for joiners, movers and leavers ensure this policy is maintained.

What security measures are in place in relation to staff working from home (or remotely) and using removable media?
Remote access is permitted for approved users only and is strictly via corporate SSL VPN, utilising 2-factor authentication, or secure Citrix connections.

Use of removable media (USB and optical ports/drives, etc.) is disabled by default via centrally managed endpoint controls. Usage is by exception and requires senior management approval. Only approved media/devices may be used and encryption is enforced.

How do you ensure staff are not a security risk?
It is Zurich’s policy to screen all candidates who are issued an employment contract, whether permanent or temporary, as part of the recruitment process – as permitted by local law or regulation.

Vetting is inclusive of: identity checks, reference and CV checks, criminal record checks, right to work in the UK compliance and credit checks. Additional vetting/assessment may be required for specific roles or responsibilities.

It is also a requirement for Zurich’s third parties/strategic suppliers to perform vetting of all their staff who are engaged on the Zurich account.

All staff (permanent, contract and temporary) are contractually required to undertake a suite of mandatory online training (including Data/Information Security, DPA, Anti-Fraud and Money Laundering, Zurich Code of Conduct) and associated knowledge confirmation assessment on joining Zurich and then annually as a minimum. Further targeted training is provided for specific roles.

Zurich also has an ongoing programme of education and awareness for all staff utilising various media and events.

All staff are contractually required to comply with Zurich policies and standards. Failure to comply with, or breaches of, security policy are subject to Zurich’s standard HR processes and may result in disciplinary action – up to and including dismissal.

How do you manage the risks associated with fraudulent email instructions?
We provide training to all staff on how to identify suspicious emails, including fraudulent or phishing emails. This includes maintaining alertness regarding unusual requests and spotting external attempts to expedite payments apparently sanctioned by senior executives but which emanate from criminals. (This criminality is known as ‘CEO fraud’.)

Employees are expected to forward all suspicious emails to our dedicated anti-phishing team on a ‘better safe than sorry’ basis, and then immediately delete these messages from their inbox. The team will respond with information either confirming the attempted fraud or malicious intent (including malware incursion) or in some instances that the email is in fact legitimate.

To maintain awareness, the anti-phishing team randomly sends emails to staff that pretend to be illicit, to check response levels. These are of course harmless, but will identify the numbers of staff who fall for trickery and require refresher training.

In addition, as email fraud attempts are unfortunately all too frequent, we wish to stress that advisers need to remain vigilant, as it is their responsibility to check with their client that any withdrawal request is actually from the client, particularly after a recent request for a change of bank account. Confirming a client’s newly emailed instructions – especially when this message appears hurried – by telephoning them on their normal phone number is good practice.

How do you ensure a payment instruction is genuine?
We have a robust anti-fraud control environment. Many of our BAU controls are in reality good anti-fraud controls too.

There are a number of controls around payments out, as our primary aim is to ensure Zurich’s assets and our customers’ assets remain safe and end up with our customer and not the fraudster, so the priority action is to verify payment requests.
Examples of controls in place:

- Risk Based Modelling (RBM) – identification of factors that influence payment out checks, e.g. level of claim, length of claim, value of claim, type of product; there is a payment out authorisation checklist in use.

- The RBM restricts third-party payees to those who can be easily verified; payee must be one of the following: 1. A Solicitor (whose name, address and client asset/money account set-up has been verified on The Law Society website and payment is made to the Solicitor’s client account. 2. Other insurers as applicable, whose name and address has been verified on the FCA website and the payee includes the full name of the insurer together with the customer name/account number. 3. The IFA, whose name, address and client account set-up has been verified on the FCA website and payment is made to the IFA’s client asset/money account. In addition, where a written request from the account/policyholder is received and third-party ID checks have been performed, payments can be made by cheque to a nursing home or school.

- Identification and Verification process.

- Checking customer signatures is a key anti-fraud control in certain scenarios.

- The party involved is contacted by a means other than email to confirm details.

- Where a change of bank account details is requested, contact is made by phone or letter to confirm if they have asked for this change. We do not use the contact details provided in the letter or email requesting the change unless these have been verified as correct.

- Where bank details are received via email, we ensure that this emanates from the legitimate email address of the party involved.

- Anti-Fraud letters – e.g. letters sent to the old and new address advising when the address was changed or double checking with the servicing agent on our Wealth Platform.

- Call handler scripts.

- Proof of existence letter.

- Reconciliations.

- Our staff minimising their work references on social media (e.g. omit role); fraudsters are known to perform online research of organisations, their CEOs and the employees in Finance departments.

Additionally, our internal training, education and awareness campaigns encourage suspicions to be reported if any of these fraud indicators are flagged:

- Overseas death and/or payment to new or foreign bank account.

- Inconsistent factors – e.g. cause of death inconsistent with lifestyle.

- Change of address and/or bank details shortly before surrender request.

- Different addresses on joint-life plans.

- Divorce/separation on joint plans followed by surrender.

- Signature forgeries.

- Numerous phone calls for information prior to surrender.

- Request to pay one party only on joint life policy.

- Customer resident in high risk country – e.g. South Africa has a known issue with postal interception, which can lead to Life Surrender Fraud.

- Customer receiving annuity at unusually old age (e.g. late 90s/early 100s).

- Language, spelling, style – is it consistent with what we would expect.

- Recipient of funds is not contactable – apparently ill, working abroad, or on holiday.

As indicated previously, on the Wealth Platform it is the advisers who are responsible for ensuring that they are dealing with their genuine clients, and acting on valid instructions from those clients. The advisers also determine the communication and view preferences for their clients. In the Platform Terms of Business, Zurich expressly informs advisers that we are not obliged to check any information they input on the Platform (and this will include changes to their client’s personal details), and also that the adviser is liable for any losses caused if they provide us with inaccurate information. We prompt advisers to check payment out requests.
Are you a member of Cifas, the UK’s fraud prevention agency?
Zurich is not a member of Cifas, however we adhere to a set of rigorous standards under which we do not tolerate fraud or financial crime, whether occurring internally or externally.

Led from the top, Zurich is committed to taking proactive steps to prevent, vigorously seek out and investigate suspected or actual incidents. Prompt and appropriate action will be taken against any individual or group perpetrating, or attempting to perpetrate, fraud against the company or its customers.

There are multiple Zurich policies, standards, procedures and controls in force which support the prevention and detection of fraud and financial crime in the UK.

The anti-fraud arrangements within Zurich are suitably designed and operate effectively. The criteria in making this assertion is the mature framework in place and that:

- There have been no significant fraud events.
- No material issues have come to light.
- The business identifies suspicions and reports them.
- Appropriate fraud risk assessment has been evident in operational assessments.
- Risks are known and remain within tolerance.
- Zurich remains transparent and accountable about our zero tolerance approach to fraud and the company goes to a high level of effort to combat internal fraud.
- Zurich has a sound business process that counters opportunistic fraud; this culture, supported by processes, ensures ethical decisions, and combats the ability to rationalise the crime, e.g. we encourage openness in the event of debt when onboarding staff.
- The FCA republished the Financial Crime Guide at the end of 2018. A benchmark review by Zurich’s Compliance team in Q1 2019 confirmed that our approach and practice to fraud matters was in keeping with the Regulator’s expectations.