AmTrust International

EU Data Protection Policy & Standards

AmTrust International

Document Reference	AIL02
Committee Owner	Executive Committee
Document Owner	European Data Protection Officer
Version Number	1.1
Next Review Date	31 December 2018

Policy History:

Version	Author(s)	Reason for Issue	Date
1.0	Andy Searle	GDPR Compliance	1 February 2018
1.1	Andy Searle	Amendment to section 7.2 to make it clear that AmTrust are likely to be independent controller, not joint.	8 June 2018

Approval History:

Version	Approved By	Date
1.0	AIL Executive Committee	23 January 2018
1.1	DPO – minor change so no ExCo approval required	8 June 2018

Contents

1. INTRODUCTION

Compliance with the General Data Protection Regulation (GDPR) and the safe and secure management of personal data is essential to AmTrust International's ("AMTRUST") continuing operation, particularly as the business expands. The modern business environment requires ever more robust systems to ensure the security of personal data, and the implementation of such systems is a vital tool in the management of our business. By keeping personal data secure, and processing it in accordance with our obligations under the GDPR, means we protect the interests of the business, its employees and its customers.

2. SCOPE

This Data Protection Policy applies to all European Union based subsidiaries of "AMTRUST", and to all staff – defined as all permanent and temporary employees, contractors, consultants and secondees.

3. PURPOSE

The purpose of this Policy is to explain Data Protection/Privacy, and to communicate the minimum standards required to help ensure compliance with the GDPR.

4. RESPONSIBILITIES

4.1 Board of Directors

The Board of Directors has overall responsibility for this Policy.

This Policy is managed by the Executive Committee on behalf of the Board.

The Board shall ensure that the Policy is reviewed at least annually so that it continues to meet AIL's business requirements, relevant regulations and remains effective in managing AIL's information security and data privacy philosophy.

4.2 Management & Employees

Management and employees at all levels are accountable for compliance with this Policy.

5. DOCUMENTATION FRAMEWORK

This Policy should be read in conjunction with the following documents:

Document	Owner
2018 Information Security Handbook	Sheryl Skolnik

6. DATA PROTECTION STANDARDS – AT A GLANCE

Principle	Requirement	Responsibility
General Good Practice	• Ultimate accountability for Data Protection compliance.	COO (AIL)
General Good Practice	• Responsible for ensuring adequate IT technical security standards, and has ultimate responsibility for the management of any information security breaches.	VP IT Operations, or local IT representatives.
General Good Practice	• Promote, monitor and advise on Data Protection compliance.	DPO & Local Data Protection reps
General Good Practice	• Develop and maintain a clear and concise Data Protection Policy that support adherence to the regulation and assist the organization with understanding its obligations.	DPO
General Good Practice	• Ensure compliance with Data Protection Policy.	All staff
General Good Practice	• Facilitate both the implementation of the Data Protection Policy within their business area, and the communication of Data Protection issues between the DPO and their business areas.	Local Data Protection reps
General Good Practice	• Know the identity of the organization's DPO.	All staff
General Good Practice	• Understand that Data Protection is everyone's responsibility.	All staff
General Good Practice	• Treat individual's data as you would want your own data to be treated.	All staff
General Good Practice	• Take extra care when receiving, sending and storing high volumes of data or sensitive data	All staff
General Good Practice	• Ensure data protection training is completed by employees.	Line Management
General Good Practice	• Ensure you complete any mandatory data protection training.	All staff
General Good Practice	• Understand the risks to customers, clients and the organization in the event of a data breach.	All staff
General Good Practice	• Know the identity of the Data Protection Authority in your jurisdiction.	All staff
General Good Practice	• Ensure that the DPO is engaged on any new projects or initiatives that involve the processing of personal data.	All staff
General Good Practice	• Ensure that any requests for information from the Police of from other law enforcement agencies or solicitors are referred to the DPO	All staff
General Good Practice	• Ensure that any Data Protection related complaints are referred to the DPO.	All staff
Fair Processing	• Advise individuals (for instance, within a Privacy Notice) as to: o How their data will be processed (collected, used, stored, & sent); o Who it will be shared with and why; o If it is to be transferred outside of the EEA; o Their rights of access & deletion; o How and where to complain;	All staff / DPO

Fair Processing	• Sensitive categories of data must be treated with extra care given the increased risks to individuals, and the DPO must be engaged if such data is to be processed.	All staff
Fair Processing	• Where CCTV is used, the DPO must be notified as there may be a requirement to advise the local regulator. Appropriate notices must be displayed, and an annual checklist needs to be completed to ensure that the CCTV is being properly used. • Any requests for access to CCTV images must be properly risk assessed and an access request checklist fully completed and retained.	Facilities/Business Units
Fair Processing	• All legal entities processing personal data must be registered with the local Data Protection Authority	DPO
Specified Purpose	• Only process data for the purpose that it was collected and only for the reasons advised to the individuals – for example, real/live customer data must not be used to test new systems, dummy, test or anonymized data must be used instead.	All staff
Adequacy	• Only use the minimum amount of personal data required to meet the aim of the activity.	All staff
Adequacy	• Remove any personal elements contained in data where possible.	All staff
Accuracy	• Keep personal data up-to-date and accurate.	All staff
Retention	• Delete any data that is no longer required, and ensure records are maintained in accordance with the records retention policy.	All staff
Rights	• Ensure you are aware of the rights of individuals and the business processes in place for them to gain access to their data – (Data Subject Access Request (DSAR)) • Ensure data is not deleted in order to not have to comply with a DSAR • Be aware of the 30-day time limit for responding to a DSAR.	All staff
Rights	• Ensure you are aware of the rights of individuals and the business processes in place for them to have their data rectified or deleted.	All staff
Rights	• Ensure you are aware of the rights of individuals and the business processes in place for them to not be marketed to.	All staff
Rights	• Do not deliver any direct marketing (to a named individual) via electronic means (email, text or SMS) without gaining consent. • Purchased marketing lists must be sourced from a reputable supplier, and be screened against AMTRUST's own marketing suppression lists as well as local marketing preference databases as appropriate.	All staff
Security	• Adhere to the company's Information Security Policies.	All staff
Security	• Adhere to the company's Secure Desk Policy.	All staff
Security	• Ensure caller's identities are validated and that they are entitled to the information. For the contact centers, at least 3 security questions must be asked.	All staff
Security	• Be careful when sending emails – minimize the volume of data, re-check the recipient's address, send externally via encryption or the use of password protected files.	All staff
Security	• Treat high volumes of data on spread-sheets or in reports with extra care, ensuring they are stored in secure locations with appropriate access restriction and are encrypted when sent outside of the organization. • Specific extra care should also be given to the recording, transmitting and storage of any bank details. Payment card details must be encrypted when stored on AMTRUST's systems or when transmitted outside of the organization, and must never be recorded on paper.	All staff
Security	• Securely dispose of personal data - paper documents must be placed in confidential waste bins or shredded.	All staff
Security	• Check printers for any uncollected data.	All staff

Security	• Report Data Protection breaches or near misses immediately to the DPO.	All staff
Security	• Computer screens MUST be locked when unattended.	All staff
Security	• Be vigilant whether inside or outside the office to any suspicious behavior or to external parties trying to obtain data.	All staff
Security	• Employees must minimize the amount of data removed from the office, and homeworkers must apply the same standards for the protection of data as in the office environment.	All staff
Security	• Ensure that the appropriate due diligence is carried out with any third party suppliers prior to starting a new relationship, and on an on-going basis.	Procurement / Vendor Management
Transfers Overseas	• Ensure that the DPO is engaged if a new initiative involves any personal data being transferred to, or accessed by, individuals located outside of the EEA.	All staff

7. CONDITIONS FOR PROCESSING PERSONAL DATA

7.1 Establishing the Data Controller / Data Processor

Before undertaking processing activities with personal data, it must be established if the entity processing the data is acting as a Data Controller or a Data Processor. A Data Controller will determine the reason for the data to be processed and that way in which it is done. A Data Processor will process data purely on the instructions of a Data Controller and will have very limited autonomy as to its use. As an example, a marketing company who is told to distribute specific marketing material, in a specific way to specific people will be acting as a Data Processor, as will many IT service providers who simply provide storage or systems solutions for another company to use.

7.2 In most cases AMTRUST will be acting as a Data Controller given the amount of decisions that they make in relation to the processing of personal data. Whilst many clients of AMTRUST will detail themselves as the Data Controller, and will have overall ownership of that data, AMTRUST are also likely be a Data Controller (independently), and as such will be legally obligated to comply with the requirements of the GDPR.

7.3 Any contract with a third party should clarify who is acting in the capacity of a Data Controller and who is acting in the capacity of a Data Processor, with advice sought from Legal and /or the DPO.

7.4 Processing Conditions

Before processing personal data, at least one of the conditions listed below must be satisfied:

- the individual has given consent to the processing;
- the processing must be necessary for the performance of a contract to which the individual is a party, or with a view to entering into such a contract;
- the processing must be necessary to comply with any legal obligation to which the Data Controller is subject, other than an obligation by contract;
- the processing is necessary for the purposes of legitimate interests pursued by the Data Controller except where the processing prejudices the rights and freedoms or legitimate interests of the individual;

- the processing is necessary in order to protect the vital interest of the Data Subject, i.e. it is literally 'a matter of life and death'.

If you are unsure what condition is fulfilled for the processing of personal data, you should contact the Data Protection Officer for guidance.

7.5 Sensitive Personal Data

Sensitive personal data is a sub-category of personal data, and is data that can cause a high degree of damage or distress to individuals if processed incorrectly. As such, this data may only be processed in limited circumstances and with stricter controls than non-sensitive personal data. Sensitive personal data is data relating to:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- the commission or alleged commission of any offence;
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings and the sentence of court in such proceedings;

7.6 If sensitive personal data is going to be processed then the Data Protection Officer must be consulted. Where sensitive data needs to be processed it should be minimized as much as possible. For example, you must only request and store details of an individual's medical history or conviction history that are specifically relevant to the risk to be insured.

8. PRIVACY NOTICES

8.1 At the point of collecting personal data from any data subject in any medium, AMTRUST must explain to individuals' certain elements of its data processing activities. This is normally achieved via a privacy notice, which would appear on AMTRUST's websites and in policy documentation.

8.2 The privacy notice must inform the customer/individual:

- Why the information is being collected;
- What legal condition AMTRUST is relying on to process the data;
- How the personal data will be used;
- Who the personal data will be shared with and for what reasons – including with suppliers and law enforcement agencies;
- Whether the personal data will be transferred outside of the EEA, and if so how it will be adequately protected;
- How long the data will be retained;
- How they will be kept informed of any changes to the privacy notice;
- Who to contact to obtain copies of their personal information;
- Who to contact in the event of a privacy complaint.

8.3 All privacy notices must be clear, transparent and take into account the GDPR and any other appropriate legal, regulatory or business requirements. Where applicable, they must tell the customer about the use of cookies or

any similar technologies used in collecting data. Privacy notices must been reviewed and updated on an annual basis as a minimum.

9. MARKETING OPT-OUTS AND OPT-INS

9.1 Right not to received marketing

An individual has the absolute right not to receive direct marketing material (that is material addressed to a specific individual). When a customer makes a request for direct marketing to cease, the request must be carried out immediately. The same right does not apply to indirect marketing (i.e. flyers or material not addressed to a specific individual) or to business to business (B2B) marketing, unless the recipient is a sole trader. Please seek guidance from the DPO before undertaking any marketing activities.

9.2 Unsolicited Marketing Messages Sent Electronically (Text/Picture/Video Messages)

It is illegal to send unsolicited marketing messages to an individual (including sole traders and unincorporated partnerships) by electronic mail (text/picture/video) unless we have the recipient's prior consent to do so. Any electronic marketing communications must contain the name of the company undertaking the marketing and must provide an easy process for the recipient to opt-out, such as an unsubscribe link.

9.3 Consent to market

A customer must give, and we need to evidence, their explicit consent to receive marketing material on any application forms, websites & mobile apps etc. Pre-ticked boxes, where a customer has to un-tick to opt-out, are non-compliant with the regulations. Ideally, marketing preferences should be channel-specific i.e. having separate opt-in boxes for mail, telephone, e-mail, and any other marketing channels. This reflects the fact that a customer may not wish to receive telephone calls, but would be happy with emails or texts.

9.4 Marketing Lists

Appropriate, accurate and up to date marketing databases should be maintained. These databases should detail which customers have consented/declined marketing, by which channels and when. These databases must be updated on a monthly basis (as a minimum), tested regularly, and must have the functionality to accept immediate ad-hoc manual changes to marketing preferences. Before issuing any marketing material, individuals must be screened against these databases to ensure we are not marketing to those who have previously opted-out. Appropriate due diligence must be carried out on any suppliers used to obtain marketing lists, to ensure they are of good standing, that data being purchased has come from a reputable source and that the individuals have provided consent to be marketed. There must also be a contract in place with any supplier who provides marketing information to AMTRUST. Any purchased lists must also be screened, as applicable, against any local marketing preference databases. For the UK this would be the Mailing Preference Service (MPS), the Telephone Preference Service (TPS), the Corporate Telephone Preference Service (CTPS), the e-mail Preference Service (eMPS), the Fax Preference Service (FMS) and SMS Preference Service (smsPS). For the Scandinavian entities this would be the NIX Register.

9.5 The DPO should be consulted prior to the initiation of any marketing initiatives to ensure compliance with both the GDPR and the Privacy and Electronic Communications Regulations (PECR).

10. WEBSITE TRACKING DEVICES

10.1 Following the Privacy & Electronic Communications Regulations 2003, if 'Web Beacons' or 'Cookies' are used for the purposes of gathering information, their use must be made clear to the customer on the website. The customer must be provided with the opportunity to withhold consent both on the initial, and any subsequent, visits to the site.

11. WORKING WITH THIRD PARTIES

11.1 Outsourcing / Third Party Processors

Where all parties in a commercial relationship are using personal data for their own purposes, and each party decides how, why and when they will use that data, then all parties are likely to be classed as Data Controllers, and each will have to comply directly with the requirements of the GDPR.

11.2 Where a third party is processing customer data on behalf of AMTRUST, and the use of the data is dictated to them by AMTRUST, then they will be acting as AMTRUST's Data Processor. As they are a Data Processor, they will have some direct liability for their processing activities under the GDPR however, most will lie with AMTRUST, and it will be AMTRUST who must ensure that the required GDPR processor obligations are place in the contract with the Data Processor.

11.3 Prior to agreeing a contract/service with a third party who will be handling personal data belong to AMTRUST or any of its clients, the DPO must be engaged to advise on any privacy and security issues.

11.4 Any due diligence / monitoring questionnaires issued to AMTRUST by third parties (insurers/clients etc.), and which include queries on Data Protection compliance must be referred to the DPO.

11.5 If information has to be sent to third parties which contains personal data, it is the sender's responsibility to ensure that;

- any transfer is made in accordance with company policies, contractual obligations and Data Protection provisions;
- all appropriate security measures are implemented to protect the information in transit, (encryption/password protection must be in place for electronic data or secure / trackable post for physical documents);
- confirmation of receipt must be obtained.

11.6 In all cases where data is transferred, employees must undertake the "Necessary" test BEFORE transferring data to third parties. That is;

- is it really necessary to transfer the data – can the aim be achieved in another way?
- is all of the data really required to be transferred – can it be minimized at all to reduce the risk?
- can the data be anonymized – can the personal identifying elements be removed?

11.7 Third Party Contracts

Relationships with third parties should be clearly defined by a contract, approved by the legal department, which should identify which party is acting as the Data Controller and which is acting as the Data Processor. It should also define the legal obligations with regard to ownership of the personal data during and at the end of the relationship, and must include an obligation on the third party to report any data security breaches to AMTRUST.

11.8 Outsourcing / Third Party Processors

Due diligence activities must be carried out on all third parties to ensure they are 'fit and proper' and can apply the expected security standards to any data provided to them. Contracts with third parties must be reviewed regularly as necessitated by regulatory, legislative and business changes. Third party relationships must be monitored, the frequency of which should relate to the inherent data security risks, to ensure adherence to the contract, and the results documented. Monitoring of third party relationships is the responsibility of the business area that owns the relationship.

12. OVERSEAS TRANSFERS OF DATA

12.1 Transfers within the European Economic Area (EEA)

Personal data can be transferred (this includes accessed) freely within the EEA (and to any countries certified as 'safe' by the European Commission) subject to the appropriate security measures being implemented to protect the data (see information security and data classification policies), and the application of the 'necessary' test (see 11.6).

12.2 Transfers outside the European Economic Area (EEA)

Personal data transferred (including being accessed) outside of the EEA, is in breach of the GDPR unless there are adequate provisions in place to ensure the security of the data. AMTRUST must ensure that the data will receive an adequate level of protection at all stages of the processing, such as implementing the EU Model Contract Clauses, which are already in place between the various AMTRUST EU entities and our US based parent company (AFSI).

12.3 In any project or new initiative, consideration must always be given to where the data is going, or being accessed from and, if this results in a transfer of personal data outside of the EEA, the DPO must be consulted prior to any transfer to ensure adequate protection is in place.

12.4 Consideration must also be given to whether there may also be any client contractual obligations on AMTRUST, not to transfer data outside of the local jurisdiction or EEA.

13. DATA PRIVACY IMPACT ASSESSMENTS (DPIA)

13.1 A DPIA is a tool, managed by the DPO, to aid the business in identifying and mitigating privacy/data protection risks associated with a new project or initiative. A DPIA should be completed (in conjunction with the DPO) at the start of a more complex, high risk or privacy intrusive initiative which involves the processing of personal data. Examples would include the introduction of new systems, the transfer of significant amounts of data, transferring data overseas or to multiple parties, the use of CCTV or any employee or customer monitoring activities.

13.2 A DPIA will provide documentary evidence to support the identification of the associated data protection/privacy risks and the appropriate mitigation. Please refer to the DPO for more details.

14. OFFICIAL BODY REQUESTS FOR DATA

14.1 Under the GDPR, various exemptions exist which allow AMTRUST (where appropriate) to process data without having to comply with a number of the normal requirements. This includes being able to disclose personal data

to other parties, such as law enforcement agencies, where there is no formal contract in place, and without the requirement to notify the individual concerned. Such activity will likely be in relation to the prevention and detection of crime or in connection with legal proceedings.

14.2 The obligations on AMTRUST to disclose personal data to the official bodies such as the Police or law firms vary between jurisdictions. For example, in the UK, there is no legal obligation to provide the information requested, unless the request is in the form of a court order. However, all requests should be referred to the DPO or local Compliance expert for advice.

- All such requests must be received in writing on official letterhead and signed by a named individual.
- NEVER PROVIDE DATA WHERE THE REQUEST HAS BEEN MADE OVER THE TELEPHONE;
- The request MUST be verified (using directory enquiries to contact the agency to ensure the request is not fraudulent);
- The request MUST be specific and not wide ranging, and should clearly stipulate what information is required and why;
- All requests MUST be logged and include details of the requesting party, the data required with justification, and what information was provided.

14.3 Disclosures required by law

AMTRUST are legally obliged to comply with certain requests for disclosure of information required by law. All such requests should be in writing and should detail the legal basis under which the information is being requested. All such requests must be referred to the DPO and the relevant Legal or Compliance department for advice.

15. DATA SUBJECT RIGHTS

15.1 Data Subject Access Requests (DSAR's)

A DSAR is a formal request by an individual for a copy of the personal information held about him/her on our records. (NOTE - Information about, or relating to, an individual such as comments about them, or opinions about them, recorded on paper, on email or other business systems could be discloseable to that individual should they submit a DSAR). The request must be received in writing, must be processed within 30 calendar days of receipt, and the information must be provided in a readable format. Any DSAR must be notified to the DPO, who will manage the request with support from the relevant business area holding the data.

15.2 Any request for information that is normally provided as part of business as usual processes, such as a copy of a letter that has already been issued by the business, or a copy of an insurance policy document does not constitute a DSAR, and the business area can simply provide the requested information. Any concerns or queries in relation to this should be referred to the DPO for advice.

15.3 Any data that has been deleted as part of normal business deletion protocols and prior to the receipt of a DSAR can legitimately be stated as having been deleted however, data must not be deleted purely as a result of receiving a DSAR, as this is a criminal offence under the GDPR.

15.4 Rights of Erasure, Rectification and Restriction of Processing and Profiling

15.5 Individuals have various data processing rights, subject to certain exemptions, which require organizations to undertake specific actions with regards to the data they hold and processed on such individuals. Such requests should be recognized as specific legal rights, and must be referred to the DPO for guidance and support.

15.6 An individual can request that an organization (data controller) deletes their information. This right is applicable if:

- the data being processed is no longer necessary for the reason it was collected;
- there is no longer a legal basis for the processing;
- the data is being unlawfully processed; or
- the data is being processed for marketing and the data subject objects.

15.7 Individuals have the right for inaccurate data or incomplete data to be rectified, and have the right to request that their data is no longer processed if:

- the data accuracy is contention;
- there is no longer a legal basis for the processing;
- the data is no longer required by the data controller; or
- the data subject objects to the processing, pending a review of the legal grounds

15.8 Individuals have the right, subject to certain exemptions, not to be subject to decision based solely on automated processing, including profiling, and human intervention may be required to review and assess any automated decision which has a legal impact on the individual.

16. PROJECTS & BUSINESS AREA DEVELOPMENTS

16.1 Projects (e.g. system implementations, the creation of new products) and business developments (e.g. the acquisition of a company) may change the scope and nature of the personal data processing. If data protection is not considered at an early stage, such initiatives may require costly alterations later on to ensure data protection compliance. It is therefore important that the DPO is made aware of forthcoming projects and business developments which may involve the processing of personal data and may recommend the completion of a Data Privacy Impact Assessment prior to any project involving data commences.

17. TRAINING

17.1 A robust and effective training strategy is the key to helping ensure data protection compliance across AMTRUST. All employees (who's details are held on Workday) must receive annual data protection training and assessment. New employees must receive this training as part of the induction program.

17.2 Contractors and temporary staff (who's details are not held on Workday) should be provided with a training pack, containing the Data Protection Policy, and asked to read and sign that they will abide by them. Business areas are responsible for ensuring that their employees complete all necessary training. The Data Protection training must be approved by the DPO.

18. ACCURACY

18.1 All personal data processed by AMTRUST must be accurate. Data is normally inaccurate if it is incorrect or misleading in any matter of fact. Data must also be kept up to date where applicable, with any necessary amendments made as quickly as possible, and the provenance of any purchased data must be retained.

19. RECORDS RETENTION

19.1 As a general rule, personal data should not be kept for longer than is necessary for the purpose for which it was being processed. Personal data records should be periodically reviewed by business area management to assess whether it is necessary to continue storing the data.

19.2 Each business area must manage their own processes for recalling and the disposal of archiving aligned to their own retention requirements. Business areas must:

- undertake periodic deletion of old electronic personal data records (including information held on network, policy and telephony systems).
- ensure paper records are periodically archived, inventories maintained and destruction dates clearly stated.

19.3 Reference should be made to AMTRUST's Record Retention Policy.

20. SECURITY AND CONFIDENTIALITY

20.1 All employees have a legal and a personal duty to keep data secure at all times, and all employees must take special care to minimize the risk of theft, loss or damage to documents & confidential information.

20.2 Each business area must ensure that its electronically stored personal data is secure. Access must be restricted to only those with a legitimate reason to see the information, and such access rights must be monitored. All employees (including contractors and temporary staff) must also ensure they adhere to the Information Security Handbook and the related I.T. Security Policies in relation to the use of laptops and system security etc. The security of data, and measures used to protect the data should be regularly reviewed.

20.3 Each business area must ensure that all personal data stored in paper form is kept secure. It must be stored in lockable cabinets with possession of keys controlled and restricted as appropriate – Please refer to the Secure Desk Policy for more information.

20.4 Contracts with off-site archive facilities must contain adequate measures to ensure security, recoverability and confidentiality. In particular, electronic data held offsite must be encrypted.

20.5 Personal data must not be transmitted by fax, unless there is a compelling business reason, in which case extreme care must be taken to ensure the fax is correctly transmitted.

20.6 Extra care must be taken when processing bank account and payment card details. The 3-digit security code/CVV/CV2 number must never be stored/retained, and care must be taken if retaining payment card numbers to ensure adequate security.

20.7 The production, distribution and storage of customer lists, such as renewal lists or bordereaux must be restricted to as few people as is necessary for processing the data. Business area management must ensure that such lists:

- are stored on restricted access network drives
- are encrypted when sent or stored outside of AMTRUST
- do not contain sensitive information or bank details unless necessary or, where they do, they are encrypted.

20.8 All employees must dispose securely of any media containing personal/confidential information. Paper documents should be placed in confidential bins or cross-shredded.

20.9 Personal data must not be stored directly on to a laptop, unless the hard drive has been encrypted, and laptops, mobile phones and other portable data storage devices must be securely locked overnight.

20.10 A security breach resulting in the loss of personal information can seriously damage individuals and the reputation of AMTRUST, who may also face regulatory/financial consequences. ANY loss of personal information must be reported immediately to the DPO.

20.11 PC screens must be locked when unattended.

20.12 Staff must be vigilant whether inside or outside the office to any suspicious behavior or to external parties trying to obtain data.

21. EMAIL SECURITY

The emailing of bulk data represents one of the biggest risks to AMTRUST in relation to data security. Before sending any data internally or externally, the data must be checked to ensure:

- Only the minimum amount of data needed is being provided – i.e. can we remove some of the personal data elements which are not required by the recipient in order to reduce the risk?

Large volumes of information or sensitive personal data must be encrypted when being sent outside of the organization, and particular care must be taken when sending email attachments such as customer lists. Email addresses should always be double checked prior to sending.

22. HOME WORKING

22.1 The use of personal data within the home should be minimized as much as possible. However, where there is a need to process, generate, store or transmit personal data in the home then the same standards for the protection of data in the office apply. Any physical (paper) records disposed of at home must be shredded, laptops securely locked away when not in use and the premises securely locked when unoccupied.

23. TEST DATA

23.1 Personal data relating to actual living individuals must only be used in systems testing where there is no suitable equivalent available, or for a final migration test. The use of such data must only be with the knowledge and consent of the DPO, and all practicable efforts should be made to anonymize the personal data used.

24. CCTV

24.1 CCTV records containing identifiable images of individuals are classed as personal data, and are therefore subject to the GDPR. The use of CCTV systems must be referred to the DPO as it may require notification to the local Data Protection Authority.

24.2 The use of CCTV cameras must be risk accessed, notices must be displayed to bring the use of any CCTV to the attention of those likely to be filmed, the images must be securely stored and made subject to a retention schedule, an annual review of CCTV use must be carried out and access to CCTV images must be tightly controlled, via an access log.

25. REGISTRATION WITH THE DATA PROTECTION AUTHORITY

25.1 In order to process personal data legally, each legal entity within AMTRUST, which is processing personal data, may need to register with the local Data Protection Authority. For the UK, this is the Information Commissioner's Office (ICO), and a failure to register is a criminal offence.

25.2 The Registration Process

In the UK, the DPO is responsible for collating the information required for each UK entity's registration and for filing the registration with the ICO. The DPO is also responsible for processing any subsequent renewals and, with assistance from the business units, for notifying of any changes or removals from the register. For other jurisdictions outside of the UK, the local compliance representative carry responsibility for the appropriate registration processes.

26. DATA PROTECTION BREACH REPORTING PROCESS

26.1 Any known, near or suspected breach of the GDPR, or a personal data compromise, must be reported immediately to the DPO. Examples would include:

- Loss of a laptop or other mobile device which contains personal data
- A malicious attack on our systems resulting in a loss of data
- Personal Data sent to the wrong person – i.e. policy docs to the wrong customer
- Theft/loss of paper records

Staff should follow the current breach reporting process, for the notification of such incidents.

26.2 The DPO will be alerted to, and keep a record of, all data protection/privacy breaches, their impact and outcome.

27. CALLER IDENTIFICATION

27.1 To help prevent any breaches of Data Protection or Confidentiality, the identity of our customers must always be verified prior to discussing or disclosing personal information with them. For any customer contact centers, who are receiving high volumes of calls to a central number then, as a minimum, customer identity must be validated by checking at least three independent data items (e.g. full name, full address and policy number). Other pieces of information that can be used include method of payment, premium paid, number of claims etc. If in any doubt as to the identity of any caller, additional validation questions must be asked. In all instances, any information provided by any customer prior to any identity checks being undertaken, must not be used as part of the security questions. Please note that checking three pieces of information is a minimum, and additional questions should be asked if there is any doubt over the identity of the caller.

28. PROFILING

28. 1 Profiling means any form of automated processing of personal data to evaluate certain personal aspects. Examples would include analyzing data to predict someone's performance at work, economic situation, health, behavior, location etc. The use of personal for such purposes must be referred to the Data Protection Officer.

29. COMPLAINTS AND QUERIES

29. 1 Business areas must ensure that all Data Protection related complaints are appropriately flagged as such, and those identified as a breach are recorded and reported (see 'Data Protection breach reporting process – Section 26).

29. 2 Many data protection complaints are often not recognized as being such, and are most likely to fall into the following categories:

- Illegal or unfair processing of the customer's data;
- Excessive information held on the customer;
- Inaccurate or incorrect information held;
- Information being retained for longer than is necessary;
- Delays in responding to Subject Access Requests, or insufficient information being supplied;
- Requests to cease processing due to the processing causing damage or distress;
- Unauthorized disclosure of the customer's information; and
- A marketing opt-out not being adhered to.

30. NON-COMPLIANCE WITH THIS POLICY

A failure to comply with this Policy may result in disciplinary proceedings. Furthermore, any breach of this Policy may result in reputational damage to AMTRUST, and a consequential loss of confidence (by customers or clients) in AMTRUST's ability to process personal data responsibly and securely.

31. FURTHER INFORMATION

Any questions regarding this Policy should be directed to the Data Protection Officer.