Information Security Policy

Introduction

Chandlers Information Security Policy applies to all business functions within the scope of the Information Security Management System and covers the information, information systems, networks, physical environment and people supporting these business functions. This document states the Information Security objectives and summarises the main points of the Information Security Policy.

Objective

The objective of Information Security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In particular, information assets must be protected in order to ensure:

- Confidentiality i.e. protection against unauthorised disclosure
- Integrity i.e. protection against unauthorised or accidental modification
- Availability as and when required in pursuance of the Organisation's business objectives.

Responsibilities

The Managing Director has approved the Information Security Policy.

Overall responsibility for Information Security rests with the Information Security Manager.

Day-to-day responsibility for procedural matters, legal compliance including data protection, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation, management reporting etc. rests with the Information Security Manager.

Day-to-day responsibility for technical matters, including technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations, rests with the Information Security Manager in conjunction with a specialised third party computer organisation.

All employees or agents acting on the Organisation's behalf have a duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay, direct to the Information Security Manager. Employees attending any location that is not occupied or owned by the Organisation must ensure the security of the Organisation's data and access their systems by taking particular care of PDAs, laptops and/or similar computers they have in their possession, together with any information on paper or other media.

The Information Security Manager is responsible for drafting, maintaining and implementing this Security Policy and similarly related policy documents as detailed in Appendix II.

As with other considerations including Quality and Health & Safety, Information Security aspects are taken into account in all daily activities, processes, plans, contracts and partnerships entered into by the Organisation.

The Organisation's employees are advised and trained on general and specific aspects of Information Security, according to the requirements of their function within the Organisation. The Contract of Employment includes a condition covering confidentiality regarding the Organisation's business.

The Information Security procedures as set out in the Organisation's Information Security Manual and the Staff Handbook detail the contractual duty of all employees. The employee signs their Contract of Employment to acknowledge acceptance of all rules, policies and procedures relating to employment within the Organisation.

Copies of this Manual, including the Risk Assessment (Annex A Appendix) are made available to all of the Organisation's employees.

Breach of the Information Security policies and procedures by the Organisation's employees may result in disciplinary action, including dismissal.

In view of the Organisation's position as a trusted supplier of enforcement agent services, particular care is taken in all procedures and by all employees to safeguard the Information Security of its service users and/or clients.

Agreements of Mutual Non-disclosure/Confidentiality are entered into, as appropriate, with third party companies.

All statutory and regulatory requirements are met and regularly monitored for changes.

Information Security Policy

A Disaster Recovery/Business Continuity Plan is in place. This is maintained, tested and subjected to regular review by the Information Security Manager.

Further policies and procedures such as those for access, acceptable use of e-mail and the internet, virus protection, backups, passwords, systems monitoring, etc. are in place, maintained and are regularly reviewed by the Information Security Manager or an appointed representative, as appropriate.

This Information Security Policy is regularly reviewed and may be amended by the Managing Director in order to ensure its continuing viability, applicability and legal compliance, and with a view to achieving continual improvement in the Information Security Systems.

GDPR

The plan overview is a seven step process detailed below:

Step 1: Gap analysis. **Step 2:** Risk analysis. **Step 3:** Project steering and resource/budget planning. **Step 4:** Implementation of a data protection structure. **Step 5:** Local Add-on Requirements. **6.** Coping with the Brexit

Step 1: Gap Analysis

- In order to assess Chandlers data protection to do's, a "gap analysis" between the current status of data protection compliance on the one side, and the obligations deriving from the GDPR on the other side, should be made. Achieving compliance with the GDPR does not only mean that new legal requirements must be met. In the course of preparing for the GDPR, potential previous non-compliance with the requirements of the EU Data Protection Directive 95/46/EC should also be remedied.
    - Thus, in a first step information with respect to current data protection practices at Company (e.g. (i) which entities / departments process what kind of data for what purposes, (ii) internal responsibilities, (iii) how are data subjects' rights safeguarded, (iv) are data protection officers implemented, (v) what IT security measures are in place etc.) should be collected (the "*Existing Data Protection Structure*").
    - In a second step the requirements deriving from the GDPR which specifically apply to the Company will have to be assessed the "*Company GDPR Requirements*").

Step 2: Risk Analysis

The efforts for implementing the GDPR requirements will be high; not all requirements can reasonably be fulfilled at once. Company will have to assess *what kind of data processing activities are of biggest risk* to (i) Company's business and/or (ii) rights of the data subjects as well as (iii) which risks most likely lead to high fines, and arrange its resources respectively. Efforts for data protection compliance should be higher for risky processing activities and lower for less risky processing activities.

Step 3: Project steering and resource/budget planning

- The GDPR implementation process requires collaboration of the Company's European entities involved, as well as awareness of the to do's on a management level at the Company. Company should assign *project responsibilities to key personnel* at the involved Company EU offices, as well as designate one *"head" project manager*, leading the project. The head project manager can also be an external advisor.

- Company should *allocate the required resources*. Planning should in particular cover (i) internal resources, such as internal personnel required for the implementation, (ii) legal costs as well as (iii) IT costs (e.g. for supporting software; IT audits etc.).

Step 4: Implementation of a data protection structure

The GDPR includes a number of additional requirements that have not existed to that extent under the EU Data Protection Directive, such as

- Strengthened **data subjects rights** (e.g. regarding *information, access and correction/deletion*; right to *data portability*; right to *object to data processing activities, "right to be forgotten"__- obligation to forward access/deletion requests to third party data recipients; higher requirements for __consent* declarations etc.),

- Strengthened **organisational requirements** (e.g. obligation to have *data processing registers* summarizing internal data processing activities; necessity of conducting *data protection impact assessments* and to appoint

data protection officers in various cases; obeying *privacy by design and by default* requirements to ensure that data processing systems are privacy-friendly; obligation to *link personal data with the purposes* for which it has been collected as well as with the *legal basis* forits processing; documentation of *data flows*; potentially draft of *deletion concepts* etc.),

- Strengthened **notification obligations** (e.g. potential obligation to *inform the data protection authorities within 72 hours of a data breach*, as well as the concerned individuals),

- Strengthened **IT/Cyber Security requirements**,

- Strengthened **contractual requirements** (stricter data processing agreements with external service providers as well as potentially within the Company-group must be concluded).

Please see the annex for more details regarding the major new requirements deriving from the GDPR. In order to cope with these new obligations, a (strengthened) data protection organisation within Company must be implemented:

4.1 Data Protection Management System The GDPR stipulates a number of requirements that are difficult to handle unless a thorough data protection management system is implemented. Such system should work group-wide, as even data protection issues in smaller Company offices may lead to high fines for the Company group as a whole.

a) Defined roles and responsibilities in the involved Company entities Company should set up a structure of *data protection responsibles* in all of its EU offices as well as a responsible head officer at the Headquarters. Respective structure should allow for (i) easily giving data protection related orders and/or advice to the involved offices ("top-down approach") as well as (ii) communication of data protection related issues to the head officer ("bottom-up" communication).

b) Procedures and concepts Many of the GDPR obligations can only be implemented in practice if respective *concepts, policies and standard operating procedures* (cumulatively "SOPs") are implemented, e.g. regarding data subjects' rights, data breach notification obligations, Data Protection Impact Assessments etc. Thus, respective SOPs should be prepared to ensure the requirements of the GDPR are met.

c) Training *Employees should be trained* about their obligations and responsibilities deriving from the GDPR.

d) Documentation Company must implement appropriate measures to *demonstrate compliance with the GDPR requirements*. Those measures shall be reviewed and updated regularly.

4.2 Data processing agreements Due to the high number of agreements to be concluded with internal and external parties, a sensible *data processing contract management* strategy will have to be implemented:

- The use of *data processors* (entities processing personal data on behalf of Company in compliance with Company's instructions) will only be permissible if thorough *data processing agreements* with the data processors are concluded. Existing agreements will have to be checked to see whether they comply with the GDPR requirements and whether they must be updated; new agreements must satisfy the high standards of the GDPR.

- In some cases, various Company entities may be regarded as *joint data controllers* if they jointly determine the purposes and means of data processing. In such cases *data processing agreements* between the involved entities generally need to be concluded.

- If personal *data is transferred from Europe to a country outside the European Union/European Economic Area, data processing agreements* must often also be concluded.

Step 5: Local Add-on Requirements

In addition to the EU-wide GDPR requirements it must be assessed whether additional national requirements exist.

- In all EU countries, additional employment-related requirements may exist regarding the processing of HR data (such as e.g. requirements to involve works councils in Germany and France or a labour office in Italy).

6: Coping with the Brexit

- Often, international company groups have their European Headquarters in the UK, which will no longer be part of the European Union in near future. Accordingly, the requirements of the GDPR may not apply directly to the Company offices in UK, and data transfers from other Company offices in the European Union to the UK office may lead to legal issues. Company will have to assess how to deal with a Brexit from a data protection perspective.

- There is a good chance that the UK will adopt privacy laws very similar to the European Union, so that the impact of a Brexit may not be too onerous. In any case, it will likely be sensible to fully apply the strict requirements of the GDPR also to UK even after a Brexit in order to limit internal bureaucracy and allow for a Europe-wide data protection structure.

Annex: Most important obligations of the GDPR

A number of new requirements are introduced by the GDPR. At a very high level, these are the most important new requirements:

1. Organisational requirements

1.1 Data Processing Registers, Art. 30 A register containing a record of processing activities under the company's responsibility must in most cases be maintained. That record shall generally contain in particular the following information:

- Name and contact details of the company and its data protection officer;

- The purposes of the processing;

- A description of the categories of data subjects and of the categories of personal data;

- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

- Transfers of personal data to a third country and the documentation of suitable safeguards;

- Envisaged time limits for erasure of the different categories of data;

- A general description of the technical and organisational security measures.

1.2 Data Protection Impact Assessment, Art. 35, 36 Where a data processing activity is likely to result in a high risk to the rights and freedoms of natural persons, the company shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations. In case the assessment indicates that the processing would result in a high risk in the absence of measures taken by the company to mitigate the risk, the supervisory authority shall be consulted.

1.3 Data Protection Officer, Art. 37-39 An independent, reliable and knowledgeable data protection officer must generally be implemented in case the company's core activities consist of

- Processing operations which require regular and systematic monitoring of data subjects on a large scale; or

- Processing on a large scale of special categories of data (e.g. health, religion, race, sexual orientation etc.) and personal data relating to criminal convictions and offences.

A group of undertakings may appoint a single data protection officer provided that such data protection officer is easily accessible from each establishment. Local laws may require the implementation of data protection officers in additional cases (likely to be the case e.g. in Germany). Thus, one global data protection officer steering data protection EU-wide may prove helpful in order to cope with differing EU-wide regulations.

1.4 Implementation of Technical and Organisational Security Measures, Art. 32 Appropriate and reasonable state of the art technical and organizational measures must be implemented in order to protect the personal data processed.

Information Security Policy

1.5 Data Breach Notifications, Art. 33, 34 In case of personal data breaches with risks to rights and freedoms of the involved data subjects, the supervisory authority shall generally be informed within 72 hours after having become aware of the breach; in case of high risks for the data subjects, these will generally also have to be informed about the breach.

1.6 Privacy by Design, Art. 25 Companies shall generally implement appropriate technical and organisational measures

- Which are designed to implement data-protection principles, such as data minimisation and integrate the necessary safeguards into the processing in order to protect the rights of data subjects (e.g. pseudonymisation).

- For ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

1.7 Representative in the EU, Art. 27 Companies subject to the GDPR but without establishment in the EU must appoint an EU representative for dealings with authorities etc.

2. Material requirements of data processing

2.1 Material requirements of data processing do not change drastically. As before, each processing of personal data (which is generally still interpreted extensively and also covers IP addresses and device identifiers) will require either valid data subject con-sent or a legal justification.

2.2 Cross-border data transfers to countries outside the European Economic Area still require additional justification (on top of 2.1), e.g. use of Privacy Shield, EU Standard Contractual Clauses or Binding Corporate Rules (or, in limited cases, consent).

3. Rights of Data Subjects, Art. 12-23

The rights of the data subjects have been strengthened. In particular, data subjects have following rights:

3.1 Information rights, Art. 12-14 Transparent and much broader notice than before must be provided to data subjects whose data is processed.

3.2 Access, deletion, rectification, restriction rights, Art. 16-19 Data subjects will generally have broad access rights with respect to their data; in some cases, they will also have the right to have their data deleted, rectified or the data processing activities restricted.

3.3 Right to Object, Art. 21-22 In some cases, data subjects have the right to object to the processing of their data on grounds relating to their particular situation.

3.4 Data Portability, Art. 20 In limited cases, data subjects may even have the right to request to receive the personal data concerning them in a structured, commonly used and machine-readable format and have the right to transmit those data to another company.

Signed: Dated: 6th May 2018

Mr C Waterman CICM, MIoD
Managing Director
Chandlers Limited