DATA PROTECTION POLICY

Octa Markets Cyprus Ltd

CIF 372/18

August 2024

Version 4

Octa Markets Cyprus Ltd is licensed and regulated by the Cyprus Securities and Exchange Commission (CySEC), with License Number 372/18
1, Ag. Zonis &Thessalonikis Corner, Nicolaou Pentadromos Center, Block: B', Office: 201, 3026, Limassol
Website: www.octaeu.com, Email: clientsupport@octaeu.com, Phone: +35725251973

Table of Contents

1. SCOPE

This Policy sets out the obligations of Octa Markets Cyprus Ltd, a company registered in Cyprus under number HE 359992, whose registered office is at 1, Agias Zonis and Thessalonikis Corner, Nicolaou Pentadromos Center, Block: B', Office: 201, 3026, Limassol ("the Company") regarding data protection and the rights of our clients, employees, and other third parties ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to clients, employees and other third parties. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. INTRODUCTION

The GDPR was approved by the European Parliament on the 14th April 2016 and effectively replaces the Data Protection Directive 95/46/EC (the "Directive") which was transposed into national law via the Processing of Personal Data (Protection of the Individual) Law 138(I)/2001. GDPR was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy. On the 31st July 2018 the Cyprus Parliament voted for the Protection of Natural Persons against the Processing of Personal Data and the Free Circulation of such Data Law 125(I)/2018 which basically provides further guidance for a more effective application of some of the articles of the GDPR.

The GDPR aims to protect all individuals in the European Union from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the Directive was established. Although the key principles of data privacy still hold true to the previous Directive, many changes have been proposed to the regulatory policies. Some of the key points of the GDPR can be found below:

- Increased territorial scope: it applies to all companies processing the personal data of data subjects residing in the European Union, regardless of a Company's location.
- Material scope: it applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.
- Severe penalties: Companies that are in breach of GDPR will be fined with heavy penalties that can be up to 4% of annual global turnover or €20 Million (whichever is greater).

- Consent: conditions for consent have been strengthened. In particular consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.
- Data Subject rights: GDPR expands the information to be provided when a data subject exercises for example the right of access, the right of erasure (right to be forgotten) while it introduces also the right of data portability.

In particular the Cyprus Investment Firms ('CIFs') as part of their client account opening procedures and ongoing obligations need to abide with the legislative framework currently in place with the Cyprus Securities and Exchange Commission ('CySEC'). In particular CIFs need to comply with their legal obligations under the AML Law (Law 188(I)/2007-2021), as amended, and the AML Directive for the establishment on the Client's economic profile and prevention of money-laundering as well as abide with the relevant record keeping obligations under the European Commission Delegated Regulation (EU) 2017/565 ('Delegated Regulation') and Law 87(I)/2017 for establishing the suitability and appropriateness of each Client based on the services offered by each CIF (Suitability & Appropriateness Tests), recordings of telephone conversations, client transactions (please refer to Section 8 and Annexes I and IV of the Delegated Regulation), FATCA and CRS:

In this respect CIFs must comply with the relevant provisions of the GDPR taking into account the current practices and legal obligation rising from the abovementioned CySEC and EU regulations. Some of the most important aspects of the GDPR, amongst others, that will affect the current procedures/polices following by CIFs are the following:

- Processing of Personal Data: personal data must be collected and processed explicitly and specifically only for the purposes that have been collected for ('purpose limitation') while the CIF must require only the information necessary in relation to the purposes for which they have been collected ('data minimisation'). In particular CIFs must abide with the relevant provision of Sections 61, 62 & 64 of AML Law and paragraphs 22, 23 & 24 of the AML Directive and gather only the relevant information and documentation related to each Client's Risk Clacification. The above also apply with respect to the record keeping obligations of CIFs rising under the Law (Law 87(I)/2017), Section 8, Annexes I and IV of the Delegated Regulation, FATCA and CRS.
- Internal Data Protection Policies and Procedures: CIFs must implement appropriate data protection policies proportionate to the their processing activities in order to be compliant with GDPR, including all relevant information and rights that each Client and employee must be aware of prior engaging and/or employed with the CIF.
- Security & Training: CIFs must take all necessary measures to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR while they must proceed and

implement appropriate data protection training to all personnel that have permanent or regular access to personal data.

3. USEFUL DEFINITIONS

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'data subject' means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

For the sake of this Policy data subject shall refer both to the employees of the Company and its Clients.

'Data Protection Authority (DPA)' means the supervisory authority of the Member State where the controller has its main establishment; in this case it means the Data Protection Commissioner.

'employee' means an individual working full-time or part time for the Company under an employment agreement, whether oral or written including temporary employees.

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'sensitive data' means the special categories of personal data defined under article 9 of the GDPR. In particular these are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

'third party' means an external organisation/person with which the Company cooperates and which is authorised directly by the Company to process personal data.

4. GDPR UNIT

The main responsibility of the GDPR Unit is to ensure that the Company is compliant with GDPR and other relevant laws and regulations. The GDPR Unit consists of the Company's Data Protection Officer (DPO). The DPO of the Company can be contacted at the following contact details:

Email: dpo@octaeu.com
Tel: +35725251973, +35799665940

The Company should publish the contact details of the DPO in the Company's Privacy Policy and communicate them to the supervisory authority. The DPO will be the point of contact between the Company and the supervisory authority on issues relating to processing of personal data, and to consult with the supervisory authority, where necessary, on any other personal data matters.

The DPO reports directly to the Company's Board of Directors. In addition, the DPO should maintain expert knowledge of data protection law and practices, as well as, other professional qualities, to ensure that the Company complies with the requirements of the GDPR and relevant data protection law(s) and regulations.

The DPO is the main contact point for employees, clients and third parties and will liaise with all relevant parties on matters of data protection and/or for the exercises of their rights (please see section 6).

The DPO should ensure that is able to perform his duties/tasks with a sufficient degree of autonomy within the Company. The DPO must not be instructed how to deal with a matter, for

example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. The autonomy of the DPO does not, however, mean that they have decision-making powers extending beyond his tasks/responsibilities as these are described below.

4.1 Responsibilities of the DPO

The DPO is entrusted with the below tasks and responsibilities:

(a) to monitor compliance with the GDPR.
(b) to ensure that documentation to demonstrate compliance with the GDPR such as policies and procedures are kept up to date. For example, the register of processing activities required under Article 30 of the GDPR. Furthermore, the DPO will plan and schedule data processing audits regularly, monitoring core activities to ensure they comply with the GDPR.
(c) collect information to identify processing activities
(d) to monitor compliance with the GDPR and other relevant laws as well as with the policies of the Company or Processors of the Company in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; and report to the Company's Board of Directors. This can take place either verbally or through a written report.
(e) inform, advise and issue recommendations to the controller.
(f) to be the point of contact for data subjects with regards to the processing of their personal data.
(g) to deal with any complaints/requests received by data subjects in relation to the processing of personal data;
(h) to inform and advise all members of staff on their obligation to adhere to the GDPR and all relevant laws and regulations when dealing with personal data;
(i) to liaise and cooperate with the supervisory authority; the DPO will be the point of contact between the Company and the supervisory authority.
(j) advise and inform on the Data Protection Impact Assessment ('DPIA'), including monitoring performance of DPIAs against the requirements of the GDPR, Article 35.
(k) to contribute to the development and maintenance of all the Company's data protection policies, procedures and processes in relation to the protection of personal data.
(l) ensure training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data.
(m) to develop/advise on formal procedures for reporting incidents (GDPR and information security-related) and investigations under Articles 33 and 34 of the GDPR.
(n) to contribute to the business continuity and disaster recovery planning process.

(o) to hold a register of all categories of processing activities carried out on behalf of the Company, acting as Controller. For this purpose, the DPO has provided the Company with the Record of Processing Activities.

In addition, the Company should seek the advice of the DPO, on the following issues amongst others:

(a) whether or not to carry out a DPIA
(b) what methodology to follow when carrying out a DPIA
(c) whether to carry out a DPIA in-house or whether outsource it
(d) what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects.
(e) whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements.

The Company should ensure that the DPO is invited to participate regularly in meetings of senior management. In particular, his presence is recommended where decisions with data protection implications are taken. All relevant information should be passed on the DPO in a timely manner in order to allow him to provide adequate advice.

The opinion of the DPO must always be given due weight. In case of disagreement, the Company should document the reasons for not following the DPO's advice. The DPO must be promptly consulted once a data breach or another incident has occurred.

The DPO is authorised to have access to all the Company's systems relating to the collection, processing and storage of personal data for the purpose of assessing the use and security of personal data. The DPO may expect the cooperation of all staff in carrying out these duties, including access to systems and records. In the event that cooperation is not being forthcoming, the DPO will report to the Company's Senior Management accordingly.

4.2 Necessary Resources

The Company should ensure that:

(a) it provides support to the DPO's function necessary to carry out their tasks and access to personal data and processing operations, and to maintain their expert knowledge.
(b) the DPO has sufficient time to fulfil his duties (e.g. conflicting priorities may result in the DPO's duties to be neglected).
(c) it provides adequate support to DPO's function in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.
(d) continuous training is provided to the Company's DPO in order to stay up to date with regard to the field of data protection.

(e) necessary access to other Company's systems relating to the collection, processing and storage of personal data

More detailed responsibilities of the DPO may be stated throughout this Policy.

5. DATA PROTECTION PRINCIPLES

All processing of personal data must be conducted by the Company in accordance with the data protection principles as set out in Article 5 of the GDPR which are described below and which are adopted by the Company. The Company's policies and procedures are designed to ensure compliance with the principles.

5.1. Personal data must be processed lawfully, fairly and transparently

5.1.1 Lawfully – identify a lawful basis on which to rely before the Company can process personal data. These are often referred to as the "conditions for processing". In particular and given the relevant provision of article 6(1) of the GDPR the Company relies on the following lawful basis:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes(e.g. used for the processing of personal data for direct electronic marketing);

(b) the processing is necessary for the performance of a contract (e.g. use of personal data for providing a service) to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

(c) the processing is necessary for compliance with a legal obligation (e.g. the processing of employees' personal data such as Social Insurance and Tax Identification Numbers for complying with the relevant legal requirements; the processing of clients' personal data for complying with the legal requirements derived from AML legislation);

(d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

5.1.2 Fairly – in order for processing to be fair, the Company has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

5.1.3 Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14 (see section 6 (a)). Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that should be provided to the data subject includes, as a minimum, the following:

(a) the identity and the contact details of the Company and, where applicable, of the Company's representative;
(b) the contact details of the DPO, as applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) the legitimate interests pursued by the Company or by a third party; where the processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party;
(e) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(f) the existence of the right to request from the Company access to and rectification, or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability (see section 6 on data subject rights);
(g) where processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal (see section 8 on consent);
(h) the categories of personal data concerned;
(i) the recipients or categories of recipients of the personal data, where applicable;
(j) the right to lodge a complaint;
(k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(l) where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
(m) any further information necessary to guarantee fair processing.

5.2. Personal data can only be collected for specific, explicit and legitimate purposes

Data must be collected for specified purposes and must not be processed for a purpose that differs from those specified as part of the Company's GDPR register of processing.

This means that the Company should:

(a) be clear from the outset why the Company collects personal data and what it intends to do with them;
(b) comply with the GDPR's fair processing requirements – including the duty to give clear notices to individuals when collecting their personal data;
(c) ensure that in the event that the Company wishes to use the personal data for any purpose that is additional to, or different from, the original purpose as this has been specified in the Privacy Policy, the new use is fair and it is clearly disclosed to the data subject.

5.3. Personal data must be adequate, relevant and limited to what is necessary for processing

(a) Each Department of the Company with the assistance of the DPO, where and as applicable, is responsible for ensuring that the Company does not collect personal data that is not strictly necessary for the purpose for which it is obtained.

(b) All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a privacy statement or link to privacy statement and must be approved in advance by the GDPR Unit. The GDPR Unit may consist only of the DPO.

5.4. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay where this is required

(a) Data that is stored by the Company must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. This shall be the responsibility of each Department to take reasonable steps to ensure the accuracy of any personal data it obtains.

(b) The DPO is responsible for ensuring with the coordination of the HR Department that all employees are trained in collecting personal data accurately and in maintaining these.

(c) The DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

(d) The DPO is responsible for responding to data subject's requests (depicted in section 6 below) **within one month**. This can be extended to a further two months for complex requests. If the Company decides not to comply with the request, the GDPR Unit must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

(e) The DPO is responsible for making appropriate arrangements so that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

5.5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

(a) Personal data will be retained in a form which permits the identification of data subjects in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

(b) The DPO must specifically approve any data retention that exceeds the retention periods as defined in the record of processing activities and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

5.6. Personal data must be processed in a manner that ensures the appropriate security

The DPO in collaboration with the IT Department and/or other relevant Departments will carry out a risk assessment taking into account all the circumstances of the Company's controlling or processing operations.

In determining appropriateness, the DPO should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or clients) if a security breach occurs, the effect of any security breach on the Company itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the DPO will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to the Company.

When assessing appropriate organisational measures the DPO will consider the following:

- The appropriate training levels throughout the Company;

- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

5.7. The Company must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires the Company to demonstrate that it complies with the principles and states explicitly that this is the Company's responsibility. The Company should be in a position to demonstrate that all six data protection principles are complied with.

The Company will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as breach notification procedures and incident response plans.

6. RIGHTS OF DATA SUBJECTS

The GDPR sets out the following rights applicable to data subjects:

a) The right to be informed

The Company should provide the following information to each data subject at the time when personal data are obtained (either obtained directly from the data subject or from a 3rd party):

i. Details of the Company including, but not limited to, the identity of its DPO;
ii. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

iii. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
iv. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
v. Where the personal data is to be transferred to one or more third parties, details of those parties;
vi. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;
vii. Details of data retention;
viii. Details of the data subject's rights under the GDPR;
ix. Details of the data subject's right to withdraw their consent at any time;
x. Details of the data subject's right to complain to the Office of the Data Protection Commissioner or to the relevant supervisory authority in their member state;
xi. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
xii. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
ii. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
iii. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

b) The right of access

Each data subject has the right to request from the Company access to the personal data that are being processed by the Company at any time by sending an e-mail or by completing a Subject Request Form and submitting same to the DPO of the Company at dpo@octaeu.com.

The Company shall provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

c) The right to rectification

The data subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate personal data concerning him or her.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

d) The right to erasure (also known as the 'right to be forgotten')

The data subject shall have the right to obtain from the Company the erasure of personal data concerning him or her without undue delay and the Company shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

i. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
ii. the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
iii. the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
iv. the personal data have been unlawfully processed;
v. the personal data have to be erased for compliance with a legal obligation to which the Company is subject.

The Company may refuse the erasure of personal data in the event that one of the following applies:

i. for compliance with a legal obligation which requires processing by Union or Member State law to which the Company is subject (i.e. for AML purposes certain personal data must be held by the Company for 5 years after the end of the business relationship with the Client).
ii. for the establishment, exercise or defence of legal claims.

e) The right to restrict processing

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

i. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

ii. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
iii. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
iv. the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

f) The right to data portability

Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, or the processing is carried out by automated means, data subjects have the right to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

In exercising his or her right to data portability the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible and by means that the Company suites appropriate (either by email or post).

Data Portability Procedure

i. The Company should inform data subjects of the existence of the right to portability at the time where personal data is obtained, through its Privacy Policy (see section 6(a) above '*Right to be informed'*).
ii. Any request should be immediately forwarded to the DPO.
iii. The Company will ask the data subject to provide evidence of their identity in the form of a current passport or ID.
iv. Where the data subject's request concerns a third party(ies), the DPO will review whether or not transmitting data to another data controller would cause harm to the rights and freedoms of other data subjects.
v. The DPO maintains a record of requests for data and of its receipt, including dates.
vi. The Company should set safeguards to ensure that the personal data transmitted are only those that the data subject has requested to be transmitted.
vii. The requested information is provided to the data subject in structured, commonly used and machine readable format that allows for the effective re-use of the data.

viii. When transmitting data to another data controller, the Company forwards the data in an interoperable format. In the event that technical impediments prohibit direct transmission, the Company should explain these impediments to the data subject(s).

ix. The Company should provide the requested information within one month from the request date. If the request is complex, the Company can extend this timeframe to (maximum) two months. The Company should inform the data subject of the reasons for the delay via e-mail within one month of receipt of the request.

x. The request does not affect the original retention period that applies to the data that has been transmitted.

g) The right to object

Data subjects have the right to object to the processing of their personal data provided that such data are processed based on legitimate interests, direct marketing (including profiling to the extent that it is related to such direct marketing), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

7. PERSONAL DATA COLLECTED, HELD AND PROCESSED

The personal data that is collected, held and processed by the Company is the following:

Data collected from clients		
Type of data	**Lawfulness of processing**	**Purpose of processing**
Client Full Name	The AML Law as amended, the AML Directive and for contractual purposes.	For the purpose of verifying the client's identity and for communication purposes
Client Contact details (home address, phone, e-mail)	The AML Law, as amended, the AML Directive and for contractual purposes	For the purpose of verifying the client's identity and for communication purposes
Personal information (Employment Status and Education level, Dependants)	The AML Law, as amended, the AML Directive and for contractual purposes	For the purpose of risk classification based on Profession, Education and Dependants
Proof of identity (copy of the ID or Passport)	The AML Law, as amended, and the AML Directive	For the purpose of verifying the client's identity

Proof of address (Utility bill / Bank Statement)	The AML Law, as amended, and the AML Directive	For the purpose of verifying the client's residence address
Client economic data (Total Estimated Annual income, Annual Spare/unused Income, Estimated Net Worth)	The AML Law, as amended, and the AML Directive	For the purpose of constructing the clients' economic profile
Source of Funds	The AML Law, as amended, and the AML Directive	Enhanced Due Diligence requirements
Tax Domicile	FATCA / CRS reporting	For the purpose of preparation and completion of FATCA/CRS reporting template
Tax Identification Number	FATCA / CRS reporting	For the purpose of preparation and completion of FATCA/CRS reporting template
Risk Warnings for residents of Spain, France and Germany	National Competent Authorities of Spain, France and Germany	Forex/CFDs are not appropriate for retail clients
Data collected from employees		
Type of data	**Lawfulness of Processing**	**Purpose of processing**
Copy of passport or ID	CySEC's Circular 025	For employment purposes
Copy of Proof of Address	CySEC's Circular 025	For employment purposes
Clear Criminal Record	CySEC's Circular 025	For employment purposes
Social Insurance Number	Social Insurance Law of 2010 (N59(I)2010)	For payroll purposes
Non-Bankruptcy Certificate	CySEC's Circular 025	For employment purposes
Tax status information	Cyprus Income Tax Law	For payroll purposes
Recruitment Information (CVs, Cover Letter, References)	Employment & Labour Laws and Regulations, Cyprus	For employment purposes
Personal Questionnaire (Employees and Directors)	CySEC's Circular 025	For employment purposes
Employee Acknowledgements (Policies. Internal Systems, Trading Platforms, Personal Transactions, CyberSecurity)	CySEC's Circular 025	For employment purposes
Performance assessments and appraisals (Salaries, positions, annual leaves)	Employment & Labour Laws and Regulations, Cyprus	For employment purposes
Telephone recordings and e-mail communication	Circular C181, CySEC	Obligations of CIFs when providing information to clients on the services and instruments offered
Processing of third parties personal data (e.g. service providers)		

Type of data	Lawfulness of Processing	Purpose of processing
A recent utility bill	Legitimate interest	For the purpose of confirming the residential address of the third party
Contact details (telephone number, e-mail address, fax number)	Legitimate interest	For communication purposes
Contact Person's Full Name & Title (Position)	Legitimate interest	For communication purposes
Business Agreement	Contract Law, Cyprus	Record keeping of Business Agreements with Business Partners
Other personal data collected from individuals (clients, prospective clients, third parties)		
Type of data	**Lawfulness of Processing**	**Purpose of processing**
Recording of telephone conversations and electronic communications	Article 17 (6) & (7) of the Law (Law 87(I)/2017) and Article 76 of the Commissions Delegated Regulation (EU) 2017/565	For monitoring purposes
Saving the users' preferences via Cookies	Consent	For marketing purposes
Personal Banking Details	The Payments Law, Central Bank of Cyprus, Cyprus	For processing payment transactions

8. SENSITIVE DATA

In addition, in the content and context of business workflow it might be possible that the Company collects or processes any of the following special categories of personal data, knows as Sensitive Data:

- Racial
- Ethnic origin
- Political opinions
- Religious beliefs
- Philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Data concerning a natural person's sex life
- Sexual orientation
- Criminal Record

- Non-bankruptcy certificate
- Other

In the course of employment and for recruitment purposes, specific *employees* personal data which are regarded as sensitive may be collected as follows:

a) Nationality: this is required for the construction of the employment contract and the legal base lies with the Contract.

b) Clean Criminal Record: this is required as per the Company's legal obligations under the legal framework it operates and under the Circular C025 issued by the regulator.

c) Non-bankruptcy certificate: this is required as per the Company's legal obligations under the legal framework it operates and under the Circular C025 issued by the regulator.

d) Biometric data: in case employees submit their national identity card, which is biometric card, it may include data such as height. The proof of identity, in this case being the National Identity Card, is required for the construction of the employment contract and the legal base lies with the Contract.

e) Tax Identification Number: For the purposes of preparation of the employment contract and payroll calculation. This comprises a legal obligation of the Company to report to the tax authorities the income tax and other contributions for each of its employees.

f) Social Insurance Number: collected and processed in the context of employment for the purpose of monthly contributions to the Social Insurance Fund. This type of information is collected under the legal base of the Social Insurance Law of 2010 (N59(I)2010) for payroll purposes.

With regards to our *Clients* and the Client On-boarding procedure, it is possible that the following information might be collected:

a) Nationality: this is displayed on the Proof of Identity, either Passport or Identity Card. The legal basis for collection and processing of this type of sensitive data is the legal obligation for KYC purposes which provides that CIFs need to know their clients and to make sure they are who they declare to be.

b) Religious beliefs: there might be cases where the national proof of identity displays the religious belief of each citizen of that given country. This type of sensitive data is being collected and processed by the Client's consent and under the legal requirement for KYC purposes which provides that CIFs need to know their clients and to make sure they are who they declare to be.

c) Biometric data: in case a client submits a national identity card (Proof of Identity), which contains MRZ lines and which consists a biometric card, it may include data such as height, colour of eyes etc. The proof of identity, in this case being the National Identity Card, is

required for the construction of the employment contract and the legal base lies with the Contract.

d) Tax Identification Number: For the purposes of preparation and completion of FATCA/CRS reporting template. This comprises a legal obligation of the Company to report to the tax authorities the data for each of its client (CRS Reporting).

Where we are asking you for sensitive personal data we will always tell you why and how the information will be used.

9. CONSENT PROCEDURE

8.1 Elements of Valid Consent

The consent of the data subject is one of the conditions for the processing of his or her personal data. The Company needs to obtain consent when no other lawful basis applies. The consent should be obtained before the Company starts processing personal data for which consent is needed.

Consent of the data subject is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Explicit consent is required for the processing of sensitive personal data.

Freely given: the data subjects have choice and control on how their personal data may be used. Consent will not be considered to be free if the data subject is unable to refuse or withdraw his consent without detriment.

Specific: the consent of the data subject should be given in relation to 'one or more specific' purposes and if there are multiple purposes, consent must be sought for each of them.

Informed: for consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. In this respect the following information is required for obtaining valid consent:

i. The controller's identity,
ii. The purpose of each of the processing operations for which consent is sought,
iii. What (type of) data will be collected and used,
iv. The existence of the right to withdraw consent,
v. Information about the use of the data for decisions based solely on automated processing, including profiling, in accordance with Article 22 (2) of the GDPR, and
vi. If consent relates to transfers, about the possible risks of data transfers to third countries in the absence of an adequate decision and appropriate safeguards (Article 49(1) of the GDPR).

With regard to item (i) and (iii), in the event where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named.

Unambiguous indication of the data subject's wishes: the GDPR requires a statement from the data subject or a clear affirmative act which means that it should always be given through an active motion or declaration.

Explicit consent: the term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. Explicit consent is needed for the processing of special categories of data (Article 9 of the GDPR).

8.2. Procedure

The Company provides a clear privacy notice wherever personal data is collected to ensure that consent is informed and that the data subject is informed of their rights in relation to their personal data.

The Company should demonstrate data subject(s) consent to the processing of their personal data or explicit consent for sensitive personal data. The Company should keep a record of consent statements received, so as to be able to show how consent was obtained, when consent was obtained and the information provided to the data subject at this time shall be demonstrable. If consent was obtained online, the Company should retain information on the session in which consent was expressed, together with the documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time. As long as the processing activity lasts (for which consent has been obtained), the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer than strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims.

The Company should be able to demonstrate that data subject(s) are informed of their right to withdraw consent as easy as giving and at any time.

10. COMPLAINTS PROCEDURE

In the event that the Company receives any complaint/request from a data subject (client, employee, service provider etc.) about how their personal data has been processed, the following procedure should be applied**:**

(a) The DPO is responsible for dealing with all complaints/requests in line with this procedure. All complaints made in relation to the scope of this procedure should be made in writing and be reported to the DPO at the following contact details:
Email: dpo@octaeu.com .

(b) The Company will update its privacy policy accordingly so as to include information in relation to how a data subject can address a complaint to the Company. The Company should have clear guidelines in its privacy policy that enable the data subject to lodge a complaint. The privacy policy should be published on the Company's website and be easily accessible from all data subjects.

(c) Data subjects are able to complain to the Company about:

- how their personal data has been processed
- how their request for access to data has been handled
- how their complaint has been handled
- disagreement with any decision made following a complaint.

(d) Upon reception of a complaint, the DPO should send a written acknowledgement (via e-mail) to the data subject, confirming reception of the complaint. The abovementioned acknowledgment should be sent within 24 working hours.

(e) The DPO shall register the complaints he received as soon as possible, in an internal register with an appropriate manner, as well as for easy reference and retrieval. In particular, upon receiving the complaint, the DPO will register the complaint directly to an internal register.

The following details have to be documented:

- the identity of the data subject who filed the complaint/request
- the date of receipt of the complaint/request
- the details of the complaint – full description (reasons for complaining)
- the investigation undertaken by the Company or the actions taken by the Company; in the event that no actions have been taken, the DPO should record the reasons for not taking actions.
- the date and in summary, the content of the reply of the Company to the said complaint/request.

(f) The DPO should ensure that complaints will be resolved within **one month** counting from the day when the written complaint has been received by the Company. That period may be extended by further two months where necessary, taking into account the complexity and number of the requests. In the event of such delay, the DPO should inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. The relevant information should be provided by e-mail.

(g) In the event that the Company does not take any action on the request of the data subject, the DPO shall inform the data subject without delay and at the latest within one month

of receipt of the request of the reasons for not taking actions and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. In doing so, the Company should provide the data subject(s) with the contact details of the supervisory authority and informs them of their right to seek judicial remedy. The relevant information should be provided in writing.

(h) The Company should inform data subjects in the privacy policy as well as in the written response sent to them that in the event that they are not satisfied with the response provided by the Company to their complaint and/or their request has not been handle within the timeframes specified above that they have also the right to lodge a complaint with the data protection authority of Cyprus as well as the data protection authority of their country of residence.

11. DATA RETENTION & DISPOSAL POLICY

Personal data as held by the Company is stored in the following ways and in the following locations:

- The Company's servers located at Velia Data Centers, in Strasburg, France, the Back-up held on Google Cloud over the web and an additional Back-up held at IS Netshop, Nicosia, Cyprus.
- Third-party servers, operated by Microsoft and Apple and located in the EEA
- Computers permanently located in the Company's premises
- Laptop computers and other mobile devices provided by the Company to its employees
- Hard-copies locked in cabinets located in the Company's premises.

The Company shall take all appropriate measures to retain personal data only for the periods identified and recorded in Company's records of processing activities. In particular the Company:

(a) shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

(b) may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

Upon the expiry of the data retention periods set out in the Company's records of processing activities, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

(a) Personal data stored electronically (including any and all backups and servers thereof) shall be deleted securely;
(b) Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely;
(c) Personal data stored in hardcopy form shall be shredded.

The Company shall make sure that all data deleted/disposed shall effectively also be deleted/disposed from any other third party/processor/sub-processor with who such data have be shared/transferred by following the procedures depicted in this Policy.

Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention should periodically be reviewed), as set out below. The Company's DPO will be responsible for reviewing the Company's Retention Policy.

When establishing and/or reviewing retention periods, the following should be taken into account:

(a) The objectives and requirements of the Company;
(b) The type of personal data in question;
(c) The purpose(s) for which the data in question is collected, held and processed;
(d) The Company's legal basis for collecting, holding and processing that data;
(e) The category or categories of data subject to whom the data relates;

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Notwithstanding the defined retention periods (as these as described in the Retention and Disposal Schedule below), certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

Responsibilities

The GDPR Unit should ensure that all personal data is collected, retained and destroyed in line with the requirements of the GDPR as well as in line with the requirements of the Company's Data Retention & Disposal Policy. The Company's DPO will be responsible for reviewing the Company's Retention & Disposal Policy.

The Accounting department is responsible for the retention of financial (accounting and tax data) records. The Accounting department should ensure that financial data are collected, retained and destroyed in line with the requirements of the GDPR.

The Company's HR Department is responsible for keeping all HR records (employees' personal data in compliance with the provisions of the CySEC's Circular C025). The HR Department should ensure that all the relevant data are collected, retained and destroyed in line with the requirements of the GDPR.

In the event that any passwords and/or cryptographic keys are required for accessing data records or stored data, the IT Department will retain this information and it will provide them upon DPO's approval.

The GDPR Unit is responsible for determining the required retention periods by type of data.

11.1 Retention and Disposal Schedule

Type of Personal Data	Purpose for which the personal data is collected, held and processed	Frequency that the data is reviewed	Retention Period/ Retention justification	Record Medium	Department responsible for the storage of data
A. INFORMATION COLLECTED FROM CLIENTS					
Client's Name and Surname	For Communication, application and AML Purposes	It is updated in the event of a marriage or divorce (if there is any change)	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM and e-mails	Back –office Department/ Compliance Department
Client Contact Details (Home Address, Phone, Email)	For Communication, application and AML Purposes	It is updated in the event of a marriage or divorce (if there is any change)	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM and e-mails	Back –office Department/ Compliance Department
Personal Information (Employment Status, Education Level, Dependants)	For Communication, application and AML Purposes	It is updated in the event of a marriage or divorce (if there is any change)	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM and e-mails	Back –office Department/ Compliance Department
Client Economic Data (Total Estimated Annual Income, Annual Spare/unused Income, Estimated Net Worth)	For AML Purposes	Annually or in case of a new transaction if it is considered necessary	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM	Back –office Department/ Compliance Department

Source of Funds	For AML Purposes	Annually or in case of a new transaction if it is considered necessary	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM	Back –office Department/ Compliance Department
Copy of the Clients' Passport or Identity card	For AML Purposes	The Company checks on a frequent basis the clients' documents to ensure that they are still valid. In case that a document is expired then the Back-office department will request an updated document.	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM and e-mails	Back –office Department/ Compliance Department
Tax Domicile/TIN	FATCA/CRS	Annually	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM and e-mails	Back –office Department/ Compliance Department
Risk Warnings	National Competent Authorities Law	Upon registration only	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM and e-mails	Back –office Department/ Compliance Department
Recent Utility Bill for verifying the client's address	For AML Purposes	Every six months	5 years (for compliance with a legal obligation - AML Requirements and for exercise or defence of legal claims)	CRM and e-mails	Back –office Department

INFORMATION COLLECTED BY THE COMPANY'S CURRENT EMPLOYEES					
Curriculum Vitae	For employment purposes	The Company may ask the employee to update his CV if it is required this necessary.	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Copy of Passport or ID	For employment purposes	The Company may request updated documents in case that they are expired.	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Clean Criminal Record	For assessing whether the employee is of good repute in line with the provisions of Circular C025.	The Company may request updated certificate every five (5) years.	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Non-bankruptcy Certificate	For assessing whether the employee is of good repute in line with the provisions of Circular C025.	The Company may request updated certificate every five (5) years.	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Tax Status Information	Cyprus Income Tax Law	Every year	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Social Insurance Number	Social Insurance Law of 2010	Upon employment	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Copy of Proof of Address	Circular C025, CySEC	Every six (6) months	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department

Personal Questionnaire Employees and Directors	Circular C025, CySEC	Upon employment	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Employee Acknowledgements (Policies, Internal Systems, Trading platforms, Personal Transactions, CyberSecurity)	Circular C025, CySEC	Every year	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Copies of academic degrees or diplomas, or/and professional qualifications	For assessing whether the employee holds academic and/or have professional qualifications and professional experience relevant to the responsibilities assigned to him, in line with the provisions of Circular C025.	The Company reviews both academic and professional qualification both at the hiring procedure and when they are acquired during the course of employment.	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Performance Assessments and Appraisals (Salaries, Positions, Annual Leaves)	Employment and Labour Laws and Regulations, Cyprus	Every year	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department
Telephone Recordings and Email communication	Circular C181, CySEC	As they incur	5 years after the end of the employment (for exercise or defence of legal claims)	e-mails, hard-copies, Company's servers	HR Department

INFORMATION COLLECTED BY CANDIDATES/ JOB APPLICANTS DURING THE RECRUITMENT PROCESS					
Curriculum Vitae	For examining whether the candidate is suitable for the position which is being applied for.	During the recruitment process.	The data are deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the individual concerned. The data may be kept for a longer period if the candidate/job applicant explicitly consents for this. OR For a period of three (3) years after the end of the process for defence against a legal claim (e.g. discrimination during the recruitment process). The Data subject(s) will be informed by the Company about future employment opportunities to similar positions only if they provide their consent to such processing.	e-mails, hard copies, Company's servers	HR Department

12. DATA SECURITY

The Company is taking all appropriate measures in relation to data security. In particular:

(a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;

(b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;

(c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

(d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

(e) All Employees are responsible for ensuring that any personal data that the Company holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Company to receive that information and has entered into a confidentiality agreement;

(f) All personal data should be accessible and processed only by the employees/departments that is necessary in order to perform their duties adequately while such data must be:

- Hard copies of personal data to be locked safely in a drawer, cabinet and/or as applicable with authorised access,
- All electronic copies of personal data must be securely stored using password and encryption, as applicable while backups should be done daily. All servers/backups must be password protected and encryption, as applicable;

(g) Care must be taken to ensure that PC screens and terminals are not visible except to authorised employees of the Company;

(h) Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with relevant procedures;

(i) Personal data may only be deleted or disposed of in line with the section 6 above;

(j) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

(k) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

(l) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;

(m) When the Company as Controller engages other agents or other third parties to process personal data on behalf of it; it should ensure that uses agents or third parties who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Processing should be governed by a contract (Article 28 of the GDPR) that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the Company.

The following technical measures are in place within the Company to protect the security of personal data:

i. All emails containing personal data must be encrypted;
ii. All emails containing personal data must be marked "confidential";
iii. Personal data may only be transmitted over secure networks;
iv. Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
v. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
vi. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
vii. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using registered or recorded delivery or a secure courier service.
viii. All personal data transferred physically should be transferred in a suitable container marked "confidential";
ix. All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

x. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
xi. Personal data must be handled with care at all times and should not be left unattended or on view;
xii. Computers used to view personal data must always be locked before being left unattended;
xiii. No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of the DPO and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
xiv. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;
xv. All personal data stored electronically should be backed up at regular intervals with backups stored onsite or offsite. All backups should be encrypted;
xvi. All electronic copies of personal data should be stored securely using passwords and encryption;
xvii. All passwords used to protect personal should be changed regularly and must be secure;
xviii. Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff should not have access to passwords;
xix. All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
xx. No software may be installed on any Company-owned computer or device without approval; and

Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the DPO, to ensure that the appropriate consent is obtained and that no data subjects have opted out.

13. DATA PROTECTION IMPACT ASSESSMENTS

The Company must perform a Data Protection Impact Assessment ('DPIA') for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

A DPIA should be carried thought the lifecycle project since this will ensure that data protection and privacy are considered and will encourage the creation and solutions which promote compliance with GDPR.

The Company is responsible for ensuring that the DPIA is carried out. The DPO is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.

The Company must also seek the advice of the DPO, where designated and this advice, and the decisions taken by the Company, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA. The Company's DPO will be responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

The Company should document its actions and decisions regarding DPIAs in order to be in a position to prove its compliance with the GDPR. For further information in relation to this, please refer to the Company's DPIA Policy.

The Company must take into account when carrying out a DPIA compliance with a code of conduct. This can be useful to demonstrate that adequate measures have been chosen or put in place, provided that the code of conduct is appropriate to the processing operation. Certifications, seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processor as well as Binding Corporate Rules (BCR), should be taken into account as well.

In this respect the Company should proceed and update its IT infrastructure in order to accommodate such a procedure and performance of such an assessment taking into account the Company's risk management processes.

The Company shall need to seek prior consultation from the Data Protection Commissioner where the DPIA reveals high residual risks and cannot be sufficiently addressed by the Company.

13.1 When to carry out a DPIA?

The Company must assess whether processing operations are likely to result in a high risk to the rights and freedoms of natural persons, and determine whether a DPIA is needed to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with the GDPR. Where a DPIA indicates that processing operations involve a high risk which the Company cannot mitigate by appropriate measures in terms of available technology and costs of

implementation, a consultation of the Data Protection Authority (DPA) should take place prior to the processing.

In particular the Company must take into account the following nine criteria when assessing whether a DPIA is needed:

a) Evaluation or scoring including profiling and predicting especially from aspects concerning the individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements
b) Automated-decision making with legal or similar significant effect i.e. aiming to take decisions on individuals.
c) Systematic monitoring
d) Sensitive data of a highly personal nature (e.g. individual political opinions)
e) Data processed on a large scale
f) Matching or combining data sets in a way that would exceed the reasonable expectations of the individual affected.
g) Data concerning vulnerable individuals. Vulnerable individuals may include children or employees. This is a criterion because of the increased power imbalance between the data subjects and the Company as the data subjects may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights.
h) Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control etc. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to data subjects' rights and freedoms.
i) When the processing in itself prevents data subjects from exercising a right or using a service or a contract. This includes processing operations that aim at allowing, modifying, or refusing data subject's access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

In most cases, the Company can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the Company envisages to adopt. However, in some cases, the Company can consider that a processing meeting only one of these criteria requires a DPIA

**__Note:__ The WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:*

a) *the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;*
b) *the volume of data and/or the range of different data items being processed;*
c) *the duration, or permanence, of the data processing activity;*
d) *the geographical extent of the processing activity*

13.2. DPIA for existing processing operations

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

A DPIA is not needed for processing operations that have been checked by the DPA or the data protection official. Consequently, the Company needs to verify whether any data processing whose conditions of implementation (scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the DPA or the data protection official and which are likely to result in a high risk then the Company is subject to a DPIA.

The Company must perform a DPIA prior to the processing and as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. DPIA should be carried throught the lifecycle project since this will ensure that data protection and privacy are considered and will encourage the creation and solutions which promote compliance with GDPR.

Prior consultation (Article 36 of the GDPR)

Where the DPIA identifies that processing of personal data will result in high risk to the data subject, in the absence of risk mitigating measures and controls, the Company consults with the Data Protection Commissioner using the following method.

- When the Company requests consultation from the Data Protection Commissioner it provides the following information:
  1) detail of the responsibilities of the Company as Controller and any other processors involved in the processing;
  2) the purposes and means of the intended processing;
  3) detail of any/all measures and controls in place/provided to protect the rights and freedoms of the data subject(s);
  4) contact details of the DPO
  5) a copy of the data protection impact assessment which carried out; and
  6) any other information requested by the Data Protection Commissioner.

14. BREACH NOTIFICATION PROCEDURE

14.1 Procedure – Detection of personal data breaches: Internal Reporting

All personnel of the Company should notify the DPO immediately if they become aware of any actual or possible personal data breach at dpo@octaeu.com . The relevant notification to the DPO is made through an internal report by using the form "**Data Breach report form".**

Heads of Departments of the Company are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

All employees of the Company must cooperate with the DPO in relation to the investigation and notification of personal data breaches.

The report (through which a breach is notified to the appointed person) should contain full and accurate details of the incident. In particular the following information should be provided to the appointed person:

- Name of the person who makes the report and his position in the Company
- Summary of the event and Circumstances (who, what, when, who etc.)
- Type and amount of personal data (kind of information included, kind of breach)
- Action taken by the person reporting the breach (if any actions have been taken)
- Action taken to retrieve data and respond to breach (if applicable)
- Action taken to minimise the risk (if applicable)

Once a data breach has been reported an initial internal assessment will be made by the Company's DPO to establish the severity of the breach. Please refer to **"Assessment of Severity of Data Breach**" Form.

Once the DPO receives an internal report, the following steps should be taken when responding to a personal data breach:

(a) conducting an investigation into the breach to assess the risks which may be associated with the breach and prepare a report (Please see ***"Assessment of Severity of Data Breach" Form***). This report will consider the following:

- How the breach occurred;
- The type of personal data involved;

- The number of data subjects affected by the breach;
- Who the data subjects are (e.g. staff, clients, suppliers etc.);
- The sensitivity of the data breached;
- What harm to the data subjects can arise? For example, are there risks to physical safety, reputation or financial loss?
- What happens if the personal data is used inappropriately or illegally?
- For personal data that has been lost or stolen, are there any protections in place such as encryption?
- Are there reputational risks from a loss of public confidence in the service the Company provides?
- Actions which have taken or proposed to be taken by the Company to mitigate the breach's possible adverse effects;
- Risk assessment and changes need to prevent further data breaches.

(b) Ensuring that the personal data breach is contained as soon as possible.
(c) Gathering and collating information from all relevant sources.
(d) Informing all interested persons within the Company of the personal data breach and the investigation;
(e) Assessing the level of risk to the Company (e.g. possibility to have a fine)
(f) Considering relevant data protection impact assessment (if applicable)

The Company's DPO will determine whether the breach is one which is required to be notified to the Data Protection Commissioner. It is not required to notify the Data Protection Commissioner regarding the breach only in case that the breach is unlikely to pose a risk to the rights and freedoms of natural persons. This means that the individual would not need to be informed about the personal data breach either as there is likely no high risk (please see section 13.7 below for further information regarding notification of the breach to the data subject). However, it should be taken into consideration that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated.

14.2 Procedure – Breach Notification: The Company to the Data Protection Commissioner where the Company acts as Controller.

This Section applies to personal data breaches affecting personal data with respect to which the Company is acting as Controller.

The Company should communicate to the Data Protection Commissioner a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person.

In particular, the Company should notify the personal data breach to the Data Protection Commissioner without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the Company is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If the data breach notification to the Data Protection Commissioner is not made within 72 hours, the Company's DPO submits it electronically with a justification for the delay.

If it is not possible to provide all of the necessary information at the same time the Company will provide the information in phases without undue further delay. The relevant information should be provided to the Data Protection Commissioner, by the appointed person, as and when it becomes available. The DPO will create a record of the reasons for any delayed notification. This record shall be stored as part of the Internal Breach Register.

The notification referred in point 13.2 above shall at least include the following information:

(a) A description of the nature of the breach.
(b) The categories of personal data affected.
(c) Approximate number of data subjects affected.
(d) Approximate number of personal data records affected.
(e) Name and contact details of the DPO
(f) Describe the likely consequences of the breach.
(g) Any measures taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
(h) Any information relating to the data breach.

The breach notification is communicated to the Data Protection Commissioner by the DPO through the completion and submission of the Data Breach Notification form which can be found here. The relevant Form is submitted to the Data protection Commissioner via e-mail at: commissioner@dataprotection.gov.cy

In the event the Data Protection Commissioner assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

The Company should keep the Data Protection Commissioner informed of changes in the facts ascertained by the Company which affect any notification made under this Section.

14.3 Procedure – Breach Notification: The Company to data subject where the Company acts as Data Controller

This section applies to personal data breaches affecting personal data with respect to which the Company is acting as a data controller.

The Company should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respective guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

Personal Data breach notifications to the affected data subjects should be made by the DPO in clear and plain language and contain at least the information and measures specified in points (e), (f) and (g) of section 13.3 above.

If the breach affects a high volume of data subjects and personal data records, the Company will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the Company's ability to appropriately provide the notification within the specified time-frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.

The Company has no obligation to notify the affected data subject of a personal data breach if:

(a) The Company has implemented appropriate technical and organisational protection measures (in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption), and those measures have been applied to the personal data affected by the personal data breach;
(b) The Company has taken subsequent measures which ensure that a high risk to the rights and freedoms of data subjects is no longer likely to materialise;

(c) It would involve disproportionate effort (in which case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner).

Providing that the DPO shall be responsible for determining whether the above applies, the DPO should create a record of any decision not to notify the affected data subjects. This record should include the appointed person's reasons for believing that the breach does not need to be notified to the affected data subjects. These details should be recorded in the Internal Breach Register.

The DPO should keep a record of all notifications, and all other communications with the affected data subjects relating to the breach.

14.4 Other Notifications

Without affecting the notification obligations set out elsewhere in this Policy, the DPO should also consider whether to notify any other third parties of a personal data breach under any other law that may apply to the Company. Notifications may be required under other associated legislation that may be applied to the Company or contract.

14.5 Procedure: Actions after the breach

After steps have been taken to resolve the data breach, the Company should review the cause of the breach and evaluate if existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring, and where applicable put a stop to practices which may lead to a data breach.

14.6 Record Keeping

Regardless of whether or not a breach needs to be notified to the Data Protection Commissioner, the DPO should keep documentation of all breaches, comprising the facts relating to the personal data breach (details concerning the breach which should include its causes, what took place and the personal data affected), its effects and consequences of the breach along with the remedial action taken by the Company. These details should be recorded in the Internal Breach Register. The relevant may be provided to the Data Protection Commissioner upon request.

The Company should also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be

documented. This should include the reasons why the DPO considers the breach is unlikely to result in a risk to the rights and freedoms of individuals. These details should be recorded in the Internal Breach Register.

Alternatively, if the DPO considers that any of the conditions describe above in Section 13.5 are met and it is not required to communicate the breach to the affected data subject(s), then the DPO should be able to provide appropriate evidence that this is the case (e.g. proof of the public communication).

Where the DPO does notify a breach to the Data Protection Commissioner, but the notification is delayed, the DPO should be able to provide reasons for this delay; in this respect documentation relating to the reasons of this delay should be kept to demonstrate that the delay in reporting is justified and not excessive.

Where the DPO communicates a breach to the affected data subject(s), he should retain evidence of such communication.

To the extent that the abovementioned records contain personal data, they will be kept by the Company for a period of six (6) years.

15. TRANSFER OF PERSONAL DATA TO A COUNTRY OUTSIDE THE EU

The Company may from time-to-time transfer ('transfer' includes making available remotely) personal data to countries outside of the EU.

This policy applies where, in accordance with the GDPR, the Company wishes to transfer personal data to third countries or international organisations outside of the EU for processing. This includes the onward transfer of personal data from a third country, or an international organisation to another third country, as well as to another international organisation within the scope of this procedure.

The transfer of personal data to a country outside of the EU shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined that ensures an adequate level of protection for personal data (Article 45(3) of the GDPR);
- In the absence of a decision from the European Commission (as stated above), the Company may transfer personal data to a third country or an international organisation only if the transfer is to a country (or international organisation) which provides

appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; standard data protection clauses adopted by the Supervisory Authority and approved by the Commission; compliance with an approved code of conduct approved by a supervisory authority; certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

In the absence of any adequacy decision pursuant to Article 45(3) of the GDPR (as stated at first bullet point above) or of appropriate safeguards as these are stated at second bullet point above (Article 46 of the GDPR), including binding corporate rules, a transfer or set of transfers of personal data to a third country or an international organisation should take place only on one of the following conditions:

- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Following the current assessment of the DPO, the Company does not transfer personal data to third countries or international organisations outside of the EU for processing. In case that such a transfer is made, the Company will implement relevant procedures to be followed for transferring personal data to countries outside the EEA.

16. TRAINING

All employees will receive training on this Policy. New employees will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the law or the Policy and procedure.

The DPO should ensure that:

- all employees with day-to- day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data (e.g. back-office and human resources department), demonstrate compliance with the GDPR.
- the persons involved in the processing of personal data are able to demonstrate competence in their understanding of the GDPR, how this is practised and implemented throughout the Company.
- the persons involved in the processing of personal data are kept up to date and informed of any issues related to personal data.
- communicate to all Employees the importance of data protection in their role and ensure that they understand how and why personal data is processed in accordance with the Company's policies and procedures.
- all security requirements related to data protection are demonstrated and communicated to Employees to the same affect.
- Employees are provided with specific training on processing personal data relevant to their individual day-to-day roles and responsibilities, and in accordance with the Company's policies and procedures.
- Employees are provided with specific training on any information security requirements and procedures applicable to data protection and the data processing within their individual day-to-day roles and responsibilities, including reporting personal data breaches.
- Employees are provided with training on dealing with complaints relating to data protection and processing personal data.
- HR Department retains records of the relevant training undertaken by each person who has this level of responsibility.

The DPO and HR Department are responsible for organising relevant training for all responsible individuals and Employees, and for maintaining records of the attendance of staff at relevant training.

In addition, this Policy as well as any updated version of this Policy will be circulated to the Company's employees in order to familiarise themselves with their obligations under the GDPR. Relevant acknowledgements that the employees have read and understood the said policy should be kept in the Company's records.

17. REVIEWING THE POLICY

The DPO should initiate at least on an annual basis the review of the Company's Policies and procedures in relation to the GDPR or in a more frequent basis, if it is considered necessary. The DPO should assess, at least, on an annual basis, the Company's internal policies and procedures and suggests proposed amendments if they are considered necessary. Any proposed updates should be approved by the Company's Board of Directors and relevant minutes should be prepared and kept in the Company's premises. Relevant records of the previous policies as well as of the proposed updates should be kept in the Company's records.

18. DOCUMENT CONTROL

The DPO is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the requirements of the GDPR.

The Company should ensure that a copy of this policy is provided to all members of staff.

Reference:	**Data Protection Policy**
Update Date:	**02.09.2024**
Approving Body:	**Board of Directors**
Date Approved:	**Q3 2024**
Version:	**4.0**
Target Audience:	**Clients, Potential Clients, Service Providers, Staff**
Author/ Lead Manager	**DPO**

19. APPENDIX 1

EXTRACT FROM THE GUIDELINES ISSUED FROM WP29 ON AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING

A. Profiling

The GDPR defines profiling in Article 4(4) as:

any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Profiling is composed of three elements:

- it has to be an automated form of processing;
- it has to be carried out on personal data; and
- the objective of the profiling must be to evaluate personal aspects about a natural person.

Article 4(4) refers to 'any form of automated processing' rather than 'solely' automated processing (referred to in Article 22). Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.

Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.

The GDPR says that profiling is automated processing of personal data for evaluating personal aspects, in particular to analyse or make predictions about individuals. The use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person.

A simple classification of individuals based on known characteristics such as their age, sex, and height does not necessarily lead to profiling. This will depend on the purpose of the classification. For instance, a business may wish to classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its clients without

making any predictions or drawing any conclusion about an individual. In this case, the purpose is not assessing individual characteristics and is therefore not profiling.

Controllers carrying out profiling will need to ensure they meet the GDPR requirements in respect of all of the above stages.

Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their:

- ability to perform a task;
- interests; or
- likely behaviour.

Example: A data broker collects data from different public and private sources, either on behalf of its clients or for its own purposes. The data broker compiles the data to develop profiles on the individuals and places them into segments. It sells this information to companies who wish to improve the targeting of their goods and services. The data broker carries out profiling by placing a person into a certain category according to their interests. Whether or not there is automated decision-making as defined in Article 22(1) will depend upon the circumstances.

B. Automated decision-making

Automated decision-making has a different scope and may partially overlap with or result from profiling. Solely automated decision-making is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, for example:

- data provided directly by the individuals concerned (such as responses to a questionnaire);
- data observed about the individuals (such as location data collected via an application);
- derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).

Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used.

Example: Imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision making process that does not necessarily involve profiling. It would, however, become a decision based on profiling if the driving habits of the individual were monitored over time, and, for example, the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations.

Decisions that are not solely automated might also include profiling. For example, before granting a mortgage, a bank may consider the credit score of the borrower, with additional meaningful intervention carried out by humans before any decision is applied to an individual.