Dechert LLP

**MEMORANDUM**

**DATE** February 21, 2017

**TO** Tim Andrews
Director, The ID Register

**FROM** Olaf Fasshauer
Kate Norman

**RE** Analysis of The ID Register's Data Privacy and Cybersecurity Practices Under EU Law

---

## 1. INTRODUCTION

1.1 When used in this Position Paper, the following terms shall have the meaning given to them in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (the **"Directive"**) or the new General Data Protection Regulation (the **"GDPR"**), as appropriate: "data controller", "data processor", "data subject", "personal data", "processing" and "sensitive personal data". These definitions are reproduced in the Glossary on page 12 of this Position Paper.

## 2. FACTUAL BACKGROUND

In this section we set out our understanding of the platform known as "The ID Register", and made available at www.theidregister.com (the **"Site"**) based on information provided by Tim Andrews and available on the Site. The legal analysis set out in paragraphs 3 to 6 is based on the assumption that the facts set out in paragraphs 2.1 to 2.5 are correct.

2.1 The ID Register is a platform which enables users to create a due diligence profile (a "**DD Profile"**) which can then be shared as required with entities needing access to the information contained in such DD Profile to conduct KYC and customer due diligence checks (e.g. banks, law firms, fund managers), avoiding the need for users to complete individual entities' KYC and customer due diligence forms on a recurring basis. A user's DD Profile may contain the following personal data:

2.1.1 Name;

2.1.2 Date of birth;

2.1.3 Address;

2.1.4 Telephone number and other contact details;

2.1.5 Drivers' licence and/or passport details;

2.1.6 Bank account details;

2.1.7 Credit or debit card details;

2.1.8 Investment information;

2.1.9 Employment information;

(together, **"DD Profile Data"**)

2.2 All DD Profile Data is provided by or on behalf of the data subject. We have assumed that where DD Profile Data is provided on behalf of the data subject (for example, by a Super User or Authorized User, as defined in the Terms and Conditions), the person providing such personal data has been properly authorised by the data subject to provide such personal data and that this authority has been properly documented.

2.3 No DD Profile is shared by The ID Register unless the user has requested that his DD Profile be connected with a third party. We have assumed that, to the extent that the sharing of a DD Profile is requested on behalf of a user, the person so requesting has been properly authorised by the data subject and such authorisation has been properly documented.

2.4 The DD Profile Data, and any other personal data that The ID Register may collect from users (such as data relating to a user's visits to the Site), are stored on Microsoft cloud servers which are physically located within the European Union.

2.5 The Site is owned by (and the DD Profile Data collected by) The ID Register (Guernsey) Limited. The following entities also have access to the DD Profile Data: The ID Register (Guernsey) Limited, The ID Register (Ireland) Limited, Apex Fund Services (U.K.) Limited, Apex Fund Services (Guernsey) Limited, Apex Fund Services (Jersey) Limited, Apex Fund Services (Ireland) Limited and Apex Fund Services (Lux) Limited. We have assumed that these entities process personal data on behalf of The ID Register (Guernsey) Limited and do not exercise control over this data or determine the purposes for which it is processed. We have prepared a draft data processing agreement between The ID Register (Guernsey) Limited and each of these entities (the "Data Processing Agreement), and this paper assumes that such agreement is duly entered into.

2.6 We have prepared a privacy policy for use on the Site which we have assumed for the purposes of this paper is in fact made available through the Site.

## 3. THE CURRENT LEGISLATIVE POSITION IN THE EUROPEAN UNION

3.1 At present, data protection in the European Union is governed by the Directive.

3.2 The Directive is not directly applicable but has been implemented by each EU Member State through its own national laws. Whilst the Directive lays down minimum requirements for Member States, some Member States have implemented stricter national laws than are required by the Directive and there is not therefore complete harmonisation across the EU. Nevertheless, we consider it useful to consider compliance with the Directive generally, as well as compliance with relevant national implementations. It is therefore necessary to consider which national implementations of the Directive apply in this instance.

3.3 From 25 May 2018 the GDPR will start to be applied across all EU Member States and replace the Directive and – within its scope – all national data protection laws in the EU Member States, bringing a level of harmonisation across the EU. It is to be seen which data protection regime will apply in the UK following its exit of the EU. Unless agreed otherwise between the EU and the UK, the GDPR will apply in the United Kingdom until such time as the United Kingdom formally exits the European Union.

3.4 As discussed with you, in this Position Paper we assess the compliance of the ID Register platform (the "**Platform**") with the Directive and GDPR. Because the Directive is addressed to EU Member States and does not apply directly to natural or legal persons we also make a compliance analysis under the national laws of the UK and Ireland. In addition we also check compliance of the Platform with the laws of Guernsey and Jersey.

3.5 Pursuant to Article 4(1) of the Directive:

> *"Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:*
>
> *(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;*
>
> *(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."*

3.6 Article 4(1) is a mandatory provision of the Directive and will therefore have been implemented into the national laws of all Member States.

3.7 In relation to the DD Profile Data, the data controller is The ID Register (Guernsey) Limited (and the privacy policy applicable to DD Profile Data states this to be the case). The ID Register (Guernsey) Limited is a company incorporated in Guernsey, which is not an EU Member State. The data controller is therefore unlikely to be "established" in an EU Member State and the Directive will not therefore apply by virtue of Article 4(1)(a).

3.8 The ID Register (Guernsey) Limited, The ID Register (Ireland) Limited, Apex Fund Services (U.K.) Limited, Apex Fund Services (Guernsey) Limited, Apex Fund Services (Jersey) Limited, Apex Fund Services (Ireland) Limited and Apex Fund Services (Lux) Limited. will be data processors of the DD Profile Data, and there should therefore be data processing agreements in place between the data controller and each of them. The entry into of the Data Processing Agreement will satisfy this requirement. The Directive will therefore render UK and Irish national law (Jersey is not an EU Member State) applicable by virtue of Article 4(1)(c) as equipment within the UK and Ireland will be being used to process the personal data.

3.9 The law of Guernsey will apply by virtue of the data controller being established in Guernsey, Guernsey law containing a provision equivalent to Article 4(1)(a) f the Directive.

Jersey law will also apply by virtue of a provision in the relevant Jersey legislation which is equivalent to Article 4(1)(c) of the Directive.

3.10 Article 4(2) of the Directive states that where the national implementation of the Directive applies in a Member State by virtue of Article 4(1)(c), the data controller is required to designate a representative established in the territory of that Member State. Accordingly, The ID Register (Guernsey) Limited as data controller will be required to appoint a representative in each of the United Kingdom and Ireland. We understand that the UK and Irish entities are to be appointed pursuant to the Data Processing Agreement. There are liability risks associated with being a representative, although this does not absolve the data controller of responsibility. Jersey law contains an equivalent provision, meaning a representative in Jersey would also be required and we understand that the Jersey entity is to be appointed pursuant to the Data Processing Agreement.

## 4. COMPLIANCE ANALYSIS UNDER THE DIRECTIVE

4.1 We set out below the text of the Articles of the Directive that are relevant to assessing compliance of The ID Register with the Directive.

Article 6 of the Directive states:

> *"(1) Member States shall provide that personal data must be:*
>
> *(a) processed fairly and lawfully;*
>
> *(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide adequate safeguards;*
>
> *(c) adequate, relevant and not excessive in relation to which they are collected and/or further processed;*
>
> *(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected of for which they are further processed, are erased or rectified;*
>
> *(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use."*

Article 7 of the Directive states:

> *"Member States shall provide that personal data may be processed only if:*
>
> *(a) the data subject has unambiguously given his consent;"*

Article 8 of the Directive states:

> *"(1) Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.*
>
> *(2) Paragraph 1 shall not apply where:*
>
> *(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent;"*

Article 10 of the Directive states:

> *"Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:*
>
> *(a) the identity of the controller and of his representative, if any;*
>
> *(b) the purposes of the processing for which the data are intended;*
>
> *(c) any further information such as*
>
> *- the recipients or categories of recipients of the data,*
>
> *- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,*
>
> *- the existence of the right of access to and the right to rectify the data concerning him*
>
> *in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject."*

Article 17 of the Directive states:

> *"1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*
>
> *Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.*
>
> *2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect*

*of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.*

*3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*

*- the processor shall act only on instructions from the controller,*

*- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.*

*4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form."*

Article 25 of the Directive states:

*"1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."*

Article 26 of the Directive states:

*"1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:*

*(a) the data subject has given his consent unambiguously to the proposed transfer;"*

4.2 The requirements arising out of each of the above relevant Articles are considered below.

4.3 <u>Fair and lawful processing: Article 6(1)(a), 7 (a), 8(1)(a) and 10.</u>

We understand that all DD Profile Data is collected, stored and transferred with the explicit consent of the data subject, which is by virtue of Articles 7(a) and 8(1)(a) sufficient for both personal data and any special categories of personal data (which may be contained in passports, or otherwise) that may be included in DD Profile Data. In addition, the information requirements are largely satisfied by the privacy policy which users are required to acknowledge that they agree to when creating a DD Profile.

We consider that the DD Profile Data is processed fairly and lawfully.

4.4 Purposes of processing: Article 6(1)(b)

As the data controller has stated the purposes for which personal data will be processed as part of the privacy policy, the data controller will be in compliance with this Article provided it doesn't exceed these purposes.

4.5 Adequacy and relevance of personal data: Article 6(1)(c)

The data controller collects various types of personal data. It is possible that the data controller may collect more personal data as part of creating a DD Profile than may be required for a particular KYC or customer due diligence exercise. However, provided that the personal data may reasonably be required for KYC, customer due diligence or other compliance tasks generally, it is our view that the data controller will be in compliance with this Article.

4.6 Accuracy of personal data: Article 6(1)(d)

We understand from the Due Diligence Pack that automatic alerts will be generated by the Site to ensure updated documents (and hence personal data) are provided by users as required. We consider that this will constitute reasonable steps to ensure that personal data processed is accurate and up to date.

4.7 Retention of personal data: Article 6(1)(e)

DD Profile Data is collected, stored and transferred at the request and with the consent of the data subject. Pursuant to The ID Register's Terms and Conditions clause 3.2 the user may terminate the licence to use the DD Profile Data at any time by deleting such data from the Site, acknowledging that The ID Register may be required to keep copies to satisfy legal or regulatory requirements. The Terms and Conditions further contemplate that The ID Register will remove such data from its systems within a reasonable time.

Assuming that the above is complied with, we are of the view that the data controller will be in compliance with this Article.

4.8 Security of processing: Article 17

The Act does not specify what will amount to "appropriate" security measures as what will be appropriate will depend very much on the particular circumstances. It is necessary to consider the state of the art and the costs of implementation against the inherent risks involved in processing the types of personal data comprised in DD Profile Data when determining whether the security measures adopted are appropriate. This analysis should be documented.

We have assumed that the security measures which The ID Register has in place are appropriate and that this requirement is therefore complied with.

4.9 International transfer: Articles 25 and 26(1)(a)

We understand that the DD Profile Data will be stored in the Microsoft Cloud located in Northern Europe. The transfer of the DD Profile Data into the cloud does not therefore raise any issues under the eighth principle.

The only circumstance we can envisage DD Profile Data being transferred out of the EEA is where a DD Profile is accessed by an institution in a non-EEA country. As all transfers of DD Profile Data are carried out with the express consent of the data subject, Article 26(1)(a) will apply such that Article 25 does not.

## 5. COMPLIANCE ASSESSMENT UNDER RELEVANT NATIONAL LAWS

### 5.1 United Kingdom

5.1.1 The United Kingdom has implemented the Directive through the Data Protection Act 1998 (the **"Act"**).

5.1.2 The Act requires that personal data be processed in accordance with the following eight data protection principles set out in Schedule 1 to the Act:

*(1)* *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –*

*(a)* *at least one of the conditions in Schedule 2 is met, and*

*(b)* *in the case of sensitive personal data, at least one of the conditions in Schedule 2 is also met.*

*(2)* *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose of those purposes.*

*(3)* *Personal data shall be adequate, relevant and not excessive in relation to the purpose of purposes for which they are processed.*

*(4)* *Personal data shall be accurate and, where necessary, kept up to date.*

*(5)* *Personal data processed for any purpose of purposes shall not be kept for longer than is necessary for that purpose or purposes.*

*(6)* *Personal data shall be processed in accordance with the rights of data subjects under the Act.*

*(7)* *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

*(8)* *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory*

*ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

5.1.3 With the exception of the sixth principle, these principles mirror the Articles of the Directive considered in paragraph 4 above and the reasoning set out in that paragraph applies equally here. The sixth principle requires personal data to be processed in accordance with the rights of the data subject under the Act. The Act gives data subjects the following rights which the data controller must honour in order to ensure compliance with this principle:

- The right of the data subject to understand what personal data of which they are the subject the data controller is processing;
- The right to prevent processing which may cause damage or distress;
- The right to prevent processing for direct marketing; and
- The right to prevent automated decision taking.

Provided the data controller honours these rights they will be in compliance with this principle.

5.2 **Ireland**

5.2.1 Ireland has implemented the Directive through the Data Protection Act 1988 (the **"Irish Act"**). The commentary in this section is based on our reading of the Irish Act and we have not taken specific advice from Irish lawyers.

5.2.2 The Irish Act requires that a data controller shall, as respects personal data kept by him, comply with the following provisions in section 2(1) of the Irish Act:

*(a) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly,*

*(b) the data shall be accurate and complete and, where necessary, kept up to date,*

*(c) the data—*

*(i) shall have been obtained only for one or more specified, explicit and legitimate purposes,*

*(ii) shall not be further processed in a manner incompatible with that purpose or those purposes,*

*(iii) shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed, and*

> *(iv) shall not be kept for longer than is necessary for that purpose or those purposes,*

*(d) appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;*

and the following set out in Section 11(1) of the Irish Act:

> *The transfer of personal data to a country or territory outside the European Economic Area may not take place unless that country or territory ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding the transfer.*

The above requirements mirror the Articles of the Directive considered in paragraph 4 above and the reasoning set out in that paragraph applies equally here.

5.3 **Jersey**

5.3.1 The commentary in this section is based on our reading of the Data Protection (Jersey) Law 2005 and we have not taken specific advice from Jersey lawyers.

5.3.2 The Data Protection (Jersey) Law 2005 mirrors the United Kingdom Data Protection Act 1998 and the commentary above at paragraph 5.1 is therefore applicable.

5.4 **Guernsey**

5.4.1 The commentary in this section is based on our reading of the Data Protection (Bailiwick of Guernsey) Law, 2001 and we have not taken specific advice from Guernsey lawyers.

5.4.2 The Data Protection (Bailiwick of Guernsey) Law, 2001 mirrors the United Kingdom Data Protection Act 1998 and the commentary above at paragraph 5.1 is therefore applicable.

## 6. THE LEGISLATIVE POSITION IN THE EUROPEAN UNION UNDER THE GDPR.

6.1 The GDPR is wider in territorial scope than the Directive. The GDPR applies to:

6.1.1 the processing of personal data in the context of an establishment of a controller **or a processor** in the EU (Article 3(1)); as well as

6.1.2 the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU where the processing activities are related to the offering of goods or services to such data subjects in the EU (Article 3(2)(a)).

Accordingly, although The ID Register (Guernsey) Limited may not be established in the EU (see paragraph 3.6 above) the GDPR will apply by virtue of Article 3(2)(a).

According to Article 27 GDPR the Guernsey entity as controller and the Jersey entity as processor will have to appoint a representative in the EU. This could be the Irish entity - because of the UK's impending exit from the EU it may not make sense any more to appoint the UK entity. Depending on the agreements around Brexit, the UK entity as processor may then itself need a representative in the EU, which again could be the Irish entity. We understand that the Irish entity has been appointed pursuant to the Data Processing Agreement.

6.2 The GDPR requires that personal data be processed in accordance with six principles set out in Article 5(1), and the data controller must be able to demonstrate compliance with these principles (Article 5(2)). The principles are broadly equivalent to Articles 6(1)(a) to (e) and 17 of the Directive. The commentary at paragraphs 4.3 to 4.8 is therefore relevant.

6.3 Legal basis for processing of DD Profile Data

The data controller must establish and document which of the legal bases set out in Article 6(1) render the processing of DD Profile Data lawful. Article 6(1)(a) provides that processing will be lawful to the extent that the data subject has given his consent. Article 9 relates to "special categories" of personal data, which is largely akin to "sensitive" personal data under the Directive. The processing of such data is prohibited unless one of the conditions in Article 9(2) applies. One such condition (Article 9(2)(1) is that the data subject has given his explicit consent to the processing of those personal data. Article 7 lays out specific conditions required for consent to be valid. The data controller must be able to demonstrate that consent has been given.

As the whole premise of The ID Register is that personal data is voluntarily given and transferred, our view is that consent may be relied on as the legal basis ensuring that the processing is lawful.

6.4 Information to be provided to data subjects

Article 13 sets out the information which the data controller must provide to the data subjects. This is similar to the information required to be provided under the Act (differences identified in **bold**):

- The identity **and contact details** of the data controller
- The identity **and contact details** of any representative of the data controller
- **The contact details of the data protection officer**

- The purposes for which the data are intended to be processed **and the legal basis for the processing**
- **The recipients or categories of recipients of the personal data**
- **information in relation to international transfer**
- **Retention period or criteria used to determine the retention period**
- **The existence of each of the rights of the data subject**
- **The existence of the right to withdraw consent at any time**
- **The right to lodge a complaint with a supervisory authority**
- **The existence of automated decision making**.

This information is largely provided in the Privacy Policy which users are required to acknowledge that they agree to when creating a DD Profile, or as part of the registration process. However, some small amendments will need to be made before the GDPR starts being enforced.

6.5 Appointment of a Data Protection Officer

Article 37(1)(b) of the GDPR requires the controller and processor to designate a data protection officer where the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.

Given that the Platform already hosts 8,000 files we think that the requirements of Article 37(1)(b) will be met and a data protection officer will be required. A single officer can be appointed for all group entities. Even if the requirements are not met, we would recommend that a data protection officer be voluntarily appointed (as contemplated by Article 37(4)) as this will enhance the credibility of the Platform.

We have assumed that a data protection officer will be appointed before the GDPR comes fully into force.

6.6 International transfers

Pursuant to Article 44 personal data can only be transferred outside the EU if the conditions of Chapter V are complied with. This requires that transfers only be made to countries in relation to which the Commission has made an adequacy finding, or the transfer is otherwise subject to appropriate safeguards prescribed in Article 46. There are adequacy decisions regarding Guernsey and Jersey.

Of relevance in this situation is that transfers outside the EU may still be made on the basis of explicit consent, provided that the data subject is informed of the possible risks of such transfer. In the present circumstances the data subject will have provided consent. In

addition, the transfer may in any event meet the requirements of Chapter V e.g. by being to a third country which is the subject of an adequacy decision.

## 7. CONCLUSION

Based on the facts, assumptions and recommendations made in paragraphs 2 to 6 above, we consider that the Platform is in compliance with:

7.1 the Directive;

7.2 its national implementations in the UK and Ireland;

7.3 the current data protection laws in force in Jersey and Guernsey; and

7.4 the GDPR.

THIS ANALYSIS IS SOLELY RENDERED FOR THE BENEFIT OF THE ID REGISTER (GUERNSEY) LIMITED, THE ID REGISTER (IRELAND) LIMITED, APEX FUND SERVICES (U.K.) LIMITED, APEX FUND SERVICES (GUERNSEY) LIMITED, APEX FUND SERVICES (JERSEY) LIMITED, APEX FUND SERVICES (IRELAND) LIMITED AND APEX FUND SERVICES (LUX) LIMITED. IT IS NOT TO BE RELIED UPON BY ANY THIRD PARTY AND DOES NOT CREATE AN ATTORNEY-CLIENT PRIVILEGE BETWEEN DECHERT LLP AND ANY SUCH THIRD PARTY.

## GLOSSARY

| Term | Directive definition | GDPR definition |
|---|---|---|
| data controller | the natural or legal person, public authority, agency or any 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 processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; | 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 processor | a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; | a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; |
| data subject | an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; | 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; |
| personal data | any information relating to an identified or identifiable natural person ('data subject'); | any information relating to an identified or identifiable natural person (‘data subject’) |
| processing | any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, | 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 |

| | | |
|---|---|---|
| | organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; | 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; |
| sensitive personal data | [No explicit definition but referred to as:<br><br>personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.] | [No explicit definition but referred to as:<br><br>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.] |