Data Protection Guidelines for Banks

May 2018

Index

Introduction

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)) will become directly applicable in all Member States, including Malta, as from 25 May 2018. It will replace the EU's Data Protection Directive 95/46/EC which is currently transposed under the Data Protection Act (Chapter 440 of the Laws of Malta), and provides for a harmonisation of the legal data protection regime throughout the EU.

The GDPR retains the core rules stipulated by previous data protection legislation and continues to regulate the processing of personal data with its goal being that of protecting individuals in this regard.

Banks are amongst the businesses that are directly affected by the GDPR, since they process significant amounts of personal data.

These Guidelines have been developed after a consultation process with the Information and Data Protection Commissioner who ascertained that the provisions of these Guidelines comply with the Regulation. This notwithstanding, such guidelines and the interpretations contained therein are without prejudice to any decision which the Commissioner may take in relation to complaints and, or any other specific data protection issues.

The purpose of these Guidelines is not to provide a detailed and comprehensive coverage of the whole Regulation. Rather, these Guidelines are intended to focus only on those sections of the Regulation which may not be entirely clear, or which could lend themselves to differing interpretations, in order that a common understanding is arrived at and a consistent interpretation is applied across the banking sector.

The Guidelines will be further developed over time, as practical issues and problems arise, and the banks' coordinated response to such issues is agreed and documented in the Guidelines. These Guidelines are also without prejudice to any further Guidelines which might be issued by the Article 29 Data Protection Working Party.

SECTION 1: Article 3 – Territorial scope

The Regulation primarily applies to the processing of personal data in the context of the activities of an establishment of a data controller or processor established in the Union, regardless of whether the processing itself takes place within the Union. Although the term "establishment" implies the effective and real exercise of the processing activity through a stable arrangement, the legal form of such arrangement is not a determining factor and could be through a branch or a subsidiary with legal personality (Recital 22).

The Regulation also applies to businesses based outside the Union that offer goods and services to, or monitor, individuals in the Union. Therefore, controllers and processors will be subject to the GDPR where the processing activities relate to:

- the offering of goods or services to individuals in the Union. It captures both free and paid for goods and services; and

- monitoring the behaviour of individuals in the Union.

In either case, the Regulation will apply when processing personal data in the Union, thus the nationality or habitual residence of those individuals is irrelevant.

These businesses will need to appoint a representative in the Union (Article 27), subject to certain limited exemptions. Such a representative must be established in a Member State where the relevant individuals are based. There is a limited exemption to the obligation to appoint a representative: where the processing is occasional, unlikely to be a risk to individuals and does not involve large scale processing of special categories of personal data. The representative should be explicitly designated by means of a written mandate of the controller or processor to act on its behalf and should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

Processors established outside the Union may also be subject to the provisions of the GDPR despite the fact that in these circumstances such processor would only be acting upon the instructions of a controller. For instance, the Regulation shall still apply if the processor established outside the Union:

- is dealing with a controller or processor based in the Union. This is because the processor would be processing personal data "*in the context of the activities of*" a controller or processor in the Union. (Article 3 (1)). In other words, when processing the personal data of data subjects who are in the Union, the provisions of the GDPR shall apply; or
- supplies services to a controller or processor who in turn supplies services to provide goods or services to, or monitor, individuals in the Union. In particular, the processor's activities arguably "*relate to*" that offering of goods or services, or monitoring (Article 3 (2)). Therefore, in some cases, processors based outside the Unionmight be subject to the provisions of the GDPR if it only deals with entities based outside the Union.

SECTION 2: Article 5 – Principles relating to processing of personal data

The guiding principles are listed under Article 5 ('*Principles relating to processing of personal data*'). These are worth recalling at the outset as any reading or interpretation of other sections must be consistent with these principles.

Article 5 of the GDPR requires a controller (the person who determines the purposes and means of processing of personal data) to ensure that:

a) personal data are processed fairly, lawfully and in a transparent manner;
b) personal data are only collected for specific, explicitly stated and legitimate purposes and are not processed for any purpose that is incompatible with that for which the information is collected;
c) personal data that are processed are adequate, relevant and limited to what is necessary in relation to the purposes of the processing;
d) personal data that are processed are accurate and, where necessary, up to date and all reasonable measures are taken to complete, correct, block or erase data to the extent that such data are incomplete or incorrect, having regard to the purposes for which they are processed;
e) personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

Personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Data on customers should not be retained for a longer period than is necessary.

In this regard, banks should be guided by the retention periods which were agreed by the Malta Bankers' Association with the Office of the Information and Data Protection Commissioner (see Annex I to these Guidelines). Furthermore, with reference to retention periods, it should be emphasised that in view of the amplified requirements to inform clients about the data processing pursuant to Articles 13 and 14, banks are required to inform clients about the intended storage periods, or at least the criteria used to determine such retention periods (e.g. by referring to the specific legal obligations laying down a mandatory retention period).

f) personal data are processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.

SECTION 3: Article 6 – Lawfulness of processing

Apart from the principles detailed in Article 5 of the GDPR, processing must also satisfy at least one of the legal criteria under Article 6. Where special categories of personal data are processed, at least one of the legal criteria under Article 9 must be satisfied (see Section 5).

Article 6 (1) makes it clear that the processing of personal data will only be lawful if it satisfies **at least one** of the following six processing conditions:

a. If the data subject has unambiguously given his consent.

This implies that the individual has given his consent to the processing for one or more specific purposes. By definition, consent must be freely given, specific and informed. The controller must keep records in order to be able to demonstrate that consent has been given by the data subject. Reference must also be made to Article 7 of the GDPR (see Section 4) which makes provision for the conditions for consent.

Where consent has been given under the Data Protection Directive (as transposed into national law by the Data Protection Act), it will continue to be valid under the Regulation to the extent that it meets the new and stringent requirements for consent provided for by the GDPR.

Controllers must ensure that their procedures to obtain consent are valid in terms of the prescriptive requirements set out in the GDPR. Procedures must also be in place to record and act upon a withdrawal of consent.

If the individual has not given his consent to the processing (as qualified above), the processing is only allowed if it falls under one of the following five headings.

b. If processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Therefore, processing in order to provide a product or service requested by a customer is perfectly permissible, and no further consent is needed.

Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

In those instances where banks process personal data which are necessary for the provision of a service requested by a client or prospective client, in line with agreed terms and conditions aimed at regulating the relationship between the client and the bank, such processing is considered legitimate under Article 6(1) (b).

Examples

(1) Various types of insurance policies (life, fire, theft, etc…) are regularly pledged to the banks as security for credit facilities extended to the pledgor himself, or to a third party for whom the pledgor is standing as surety.

In order to complete and validate their security, the banks give notice of such pledges to the insurance companies concerned, also requesting the current surrender value / expected maturity value of life policies, confirmation that the premium has been paid to date, notification by the insurance company to the bank in the event of future premium remaining unpaid, and confirmation that there are no existing prior-ranking charges on the policies.

Processing of the above data at the time that a policy is pledged, and periodically thereafter, is essential for the banks to be able to look at the pledged policies as effective security, and such processing should not require the pledgor's specific consent as the pledgor himself is a party to the pledge agreement. Moreover, such processing 'is necessary for a purpose that concerns a legitimate interest of the controller' (see Article 6 (1) (f)).

The position of the insurance companies, when responding to such requests by the banks, is likewise covered by Article 6 (1) (f) (see below).

(2) In the course of their business, banks discount or accept as security Bills of Exchange which are payable to, or have been endorsed in favour of, their customers.

Bills of Exchange are negotiable instruments, and by their very nature contain details of various third parties, including the drawer, drawee, beneficiary and subsequent endorsees, **all of whom are parties to the Bill of Exchange**. As such, no notification to any of these parties is deemed necessary when banks are processing Bills of Exchange handed to them by their customers for discounting or as security for credit facilities.

c. If processing is necessary for compliance with a legal obligation to which the controller is subject.

This applies in situations involving data processing which is carried out to comply with statutory obligations imposed by law on controllers, e.g. reporting to the tax authorities, or reporting of suspicious transactions under the Prevention of Money Laundering Regulations. Only legal obligations under Union or national law will satisfy this condition.

Processing is necessary for compliance with a legal obligation to which the controller is subject.

(1) This covers processing due to statutory duties imposed by law such as reporting or due diligence obligations arising from the Prevention of Money Laundering Regulations, reporting to tax authorities in terms of FATCA or other agreements or laws.

(2) Banks must necessarily process and maintain data relating to attachment / freezing orders issued under the Prevention of Money Laundering legislation, persons who have been interdicted, garnishee orders and any other order issued by a Court of law or any other competent authority.

(3) Banks are required, under the Prevention of Money Laundering legislation, to process and retain copies of customers' identification documents.

Where the information is directly requested from the clients, banks shall inform clients that such data are being requested due to its statutory requirements.

In other instances, where banks process personal information as part of their statutory or legal obligations, and such data are not directly obtained from the client, banks are exempt from notifying the client where the individual already has the information, or where processing or disclosure is expressly laid down by law to which the bank is subject and which provides appropriate measures to protect data subject's rights.

d. If processing is necessary in order to protect the vital interests of the data subject or of another natural person.

The Regulation does not define 'vital interests'. This is typically limited to processing needed for medical emergencies.

e. If processing is necessary for the performance of a task that is carried out in the public interest or in the exercise of official authority vested in the controller

This article may also be utilised when processing of personal data is necessary for the performance of an activity that is carried out in the public interest. The notion of public interest is developed mainly through case law.

f. If processing is necessary for a purpose that concerns a legitimate interest of the controller or of a third party, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject, in particular where the data subject is a child.

This principle sets up a balance between two interests. Thus, if the consequences of the processing are detrimental to a particular individual, and there are no other '*necessary*' grounds that would take precedence, then one would expect the individual's interests to override the controller's interests in the continuation of the processing.

Processing is necessary for a purpose that concerns a legitimate interest of the controller or of a third party, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject, in particular where the data subject is a child.

(1) Lending is one of the banks' major business activities and 'Loans and Advances to Customers' normally account for a large proportion (+50%) of their total assets. Such business carries significant potential credit risks which banks must manage with great caution and prudence in the interests of their shareholders, customers, staff and the financial services industry in general.

For this reason, banks consider it vital and certainly in their legitimate interest to maintain relevant information to alert their lending officers to the risks of making new or further advances to certain individuals who, on the basis of past experience, clearly do not qualify for such new or additional lending.

Typically, the nature of the information maintained would include details of:

- Defaulting borrowing customers, where recovery of the debt is doubtful or very problematic.
- Customers whose current account or payment card account has been misconducted.

- Individuals (both customers and non-customers) whose application for credit facilities has been declined by any branch of the bank.
- Individuals who have been declared bankrupt, or in respect of whom bankruptcy proceedings are in course.
- Drawers of cheques returned unpaid to the bank by other banks (on which the cheques are drawn) with answer 'Refer to Drawer'.
- Drawees (both customers and non-customers) of Bills of Exchange which were discounted /accepted as security by the bank, and which were not honoured when payment fell due.
- Individuals (both customers and non-customers) who are known / suspected of having forged or stolen cheques, or to be in possession of forged or stolen cheques. Such information would need to be supported by a police report or other reliable sources (e.g. the bank's security officer who would have conducted the necessary investigations).
- Information received from Credit Reference Agencies, the Central Credit Register maintained by the Central Bank of Malta and from other reference databases.

For obvious reasons, banks may need to retain such information even after termination of their banking relationship with the customers concerned. However, the banks shall review all such information periodically to ensure that it is correct/ up-to-date, and judiciously consider deletion of such information in those cases where retention of the data is no longer deemed necessary.

(2) The processing of personal data by the banks for the purposes of pledged insurance policies and any notice of pledge which is issued to insurance companies is covered not only by Article 6 (1) (b) but also by Article 6 (1) (f).

This interpretation is supported by the wording of Article 6 (1) (f) which permits the processing of personal data when such processing "...*is necessary for the purposes of the legitimate interests pursued by the controller or* ***by a third party***. . ." (i.e. the banks in the case of pledged policies).

It is certainly in the banks' legitimate interest to be informed that a pledgor has not paid his premium, since this would enable the bank to pay the premium itself (as it is legally entitled to do) and thus preventing the lapse of the policy which could be extremely detrimental to the bank. Likewise, a bank has a legitimate interest to ascertain the value of the security against which it is allowing credit facilities to a debtor.

(3) The 'Know Your Customer' principle is particularly relevant to bank business, and banks must seek to have maximum knowledge of a prospective customer's affairs, including details of his background, means, etc. This is also necessary for banks to comply with the due diligence procedures which are called for under the anti-money laundering legislation (see Article 6 (1) (c) above).

While the processing which is necessary as part of the 'Know Your Customer' and due diligence process may be carried out in view of the legal obligations to which banks are subject and also for purposes concerning legitimate business interests, a distinction needs to be drawn between instances where processing is necessary in view of such obligations or for purposes involving core business activities of banks, and other situations where the

processing is intended to provide value-added services aimed at specific clients based on their unique customer profile. When collecting and processing personal data as part of their due diligence, Banks should take into account the principles contained in Article 5 of the GDPR, more specifically the purpose limitation principle.

In this regard, where customers are subject to profiling aimed at targeting them with specific customised offers, products or services, similar profiling would require the consent of such persons.

Other market segmentation or profitability analyses, carried out for the purposes of enabling the bank to render an overall better service to its customers, may be considered in the legitimate interest of banks.

The Necessity Factor

The use of the word 'necessary' in Article 6 (b)–(f) should not be overlooked. This word implies that under these provisions, processing is permitted only if the purpose is attained by means of such processing.

Why processing conditions really matter

Under the GDPR, it is important to clearly understand and identify the legal ground for the processing of personal data. In view of the prescriptive nature of consent under the GDPR, relying on consent as a legal basis will only be possible in limited circumstances where all the conditions required for a valid consent (as outlined in Section 7), are fulfilled.

Other processing operations where banks cannot rely on consent as legal ground for processing.

CCTV

Video surveillance constitutes processing of personal data. Persons within the monitored area must be aware that they are being monitored. For this purpose banks should affix appropriate signs, which are clearly visible, on the façade of their premises. The signs should clearly state the purpose of processing.

Normally, CCTV recordings within a bank are used for security purposes. It is not excluded, however, that available CCTV recordings could be used by a bank for the purpose of an internal investigation involving a member(s) of its staff provided, however, that the staff concerned had been made aware that they could have been recorded on the bank's monitoring system.

CCTV recordings shall not be retained for a period longer than is necessary. In so far as customer-facing footage is concerned, such period shall not be longer than 30 days, provided that where specific footage is used in connection with an investigation, a copy of the relevant extract from the recordings may be retained as evidence until the case is concluded. Back-office operations footage does not as a rule capture the faces of the employees, but only their hands and the cash handling process. In such cases, the footage of back-office operations can be kept for a period which is not longer than 90 days.

CCTV's in the form of pin-hole cameras are used by banks on ATM's. In this case, since such monitoring is carried out mainly for the prevention of crimes, no signs indicating the presence of the pin-hole camera need be affixed to the ATM.

Telephone Recordings

Recordings of telephone conversations constitute processing of personal data. Callers and staff should therefore be advised beforehand if such recording is being carried out. This requirement is also applicable to the recording of outbound calls. In similar cases, staff members shall, prior to proceeding with the telephone call, inform the recipient that the call will be recorded.

The retention period for telephone recordings varies depending on the purpose for processing such recordings. As a general rule, telephone recordings ought not be kept for a period longer than thirty (30) days. However, those telephone recordings which have a bearing on the legal or contractual obligations of the bank can be kept for the term of the contract or for as long as the legal obligation subsists.

In the case of all telephone recordings retained for training purposes, the identity of the person and as much as possible the voice of the person ought to be masked.

Monitoring of Electronic Mail and Internet Usage

In accordance with the Article 29 Data Protection Working Party's Opinion 2/2017 on data processing at work (adopted on 8 June 2017), when processing data relating to the use of technologies by employees, banks as employers should always consider whether:

- The processing activity is necessary, and if so, the legal grounds that apply;
- The proposed processing of personal data is fair to the employees;
- The processing activity is proportionate to the concerns raised; and
- The processing activity is transparent.

Where it is the bank's policy to monitor staff e-mails and Internet usage, this policy should be clearly stated and communicated to all staff. It is recommended that in these instances banks adopt a read and sign approach.

Further detailed guidance on the monitoring by employers of their employees' use of technology at the workplace or outside the workplace can be accessed by reference to the Article 29 Data Protection Working Party's Opinion 2/2017 on data processing at work – see Annex II to these Guidelines.

SECTION 4: Article 7 – Conditions for consent

Article 7 of the GDPR stipulates the following conditions for consent:

(i) Plain language

A request for consent must be in an intelligible and easily accessible form in clear and plain language.

(ii) Separate

Where the request for consent is part of a written form, it must be clearly distinguishable from other matters.

(iii) *Affirmative action*

The consent must consist of a clear affirmative action. Inactivity or silence is not enough and the use of "pre-ticked boxes" is not permitted.

(iv) Consent to all purposes

If the relevant processing has multiple purposes, consent must be given for all of them. For example, in the context of the provision of a service, it is not possible to rely on the consent obtained in this regard if direct marketing is envisaged. A separate consent must be obtained for the latter.

(v) No detriment

Consent will not be valid if the individual does not have a genuine free choice or if it is detrimental to him/her should he/she refuse or withdraw consent.

(vi) No power imbalance

Consent might not be valid if there is a clear imbalance of power between the individual and the controller.

(vii) Unbundled consent

"Bundle Consent" is not permitted. Where different processing activities are taking place, consent is not valid unless the individual can consent to them separately.

(viii) Not tied to contract

Consent is not valid if it is a condition for the performance of a contract.

(ix) Withdrawable

The individual can withdraw consent at any time and prior to giving consent, the data subject shall be informed thereof. For a data subject to withdraw his or her consent, it should be as easy as it was at the stage when the consent was given.

(x) Explicit

When special categories of personal data or when transferring personal dataoutside the Union, the consent must be explicit. This entails a degree of formality, for example, the individual being requested to tick a box containing the express word "*consent*".

SECTION 5: Article 9 – Processing of special categories of personal data

Article 9 of the GDPR deals with the processing of 'special categories of personal data' and places much stronger controls when processing such data.

'*Special categories of personal data*' are in terms of the GDPR (Article 9 (1)) "*personal data revealing race or ethnic origin, political opinions, religions or philosophical beliefs, or trade union membership*" as well as "*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*"

Any processing of special categories of personal data must satisfy **at least one** of the following conditions:

a. Explicit consent

The individual has given explicit consent.

b. Legal obligation related to employment

The processing is necessary for a legal obligation in the field of employment and social security law or for a collective agreement.

c. Vital interests

The processing is necessary in order to protect the vital interests of the individual or of another natural person. This is typically limited to processing needed for medical emergencies.

d. Not for profit bodies

The processing is carried out in the course of the legitimate activities of a not-for-profit body and only relates to members or related persons and the personal data is not disclosed outside that body without consent.

e. Public information

The processing relates to personal data which is manifestly made public by the data subject.

f. Legal claims

The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g. Substantial public interest

The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law.

h. Healthcare

The processing is necessary for healthcare purposes and is subject to suitable safeguards.

i. Public health

The processing is necessary for public health purposes and is based on Union or Member State law.

or

j. Archive

The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and is based on Union or Member State law.

Special categories of personal data

Banks may process special categories of personal data in relation to employees. Such data is usually obtained from the employees themselves. When the processing of special categories of data is necessary for the bank to carry out its obligations and exercise specific rights in the field of employment and social security and social protection law in so far as it is authorised by law, the employees' explicit consent is not required for the processing of such data. Strict levels of access and access rights apply in relation to special categories of personal data, hence allowing access only to those officials who must essentially process said data in the performance of their duties.

Examples of special categories of personal data:

(1) Data concerning cause of illness

As a rule, whenever a bank employee reports that he or she is unable to attend work due to illness, the bank cannot request such employee to divulge the cause of his or her illness. That said, banks may still send a medical practitioner and subject an employee to a medical check-up, provided that the cause of illness is only processed by such practitioner, and the bank will only receive confirmation as to whether the person was unfit for work. Should an employee repeatedly report sick, or in the event of long-term illness, the bank can request the medical practitioner to draw up a brief report on the employee, including where strictly necessary general information on the employee's medical condition, in order to enable the assessment of his working capacity by the employer (vide Article 9 (2) (h)). The employee should be informed accordingly.

(2) Pre-employment medical assessment

It is permissible for banks to request employees selected to be employed by the bank, following a recruitment process, to attend a medical examination in order for a medical professional to ascertain that they are fit for work. It is sufficient for the certificate issued by the medical professional to state that the prospective employee is fit for work, with no further details as to the diagnosis divulged therein. Should the certificate not give the

prospective employee a clean bill of health, banks may request further explanations from the medical professional who would have assessed the candidate.

Should a candidate for a post not be recruited further to such medical assessment, the bank should only retain records of such medical assessment or diagnosis for a period of four months which is the legal period within which the candidate could contest the non-engagement by the employer (vide Article 30 (1) of the Employment and Industrial Relations Act, Chapter 452 of the Laws of Malta). Should the bank decide to engage the employee despite the negative diagnosis, the medical records relating to such an employee can be retained in the file should the medical condition have an impact on the working environment and in order to safeguard the health and well-being of the employee himself/herself. In view of the sensitive nature of the data, this should be subject to strict security measures and shall be kept separate from other HR records which are likely to be processed as part of routine HR practices (e.g. payroll, CV, employment contract, benefits).

SECTION 6:

Article 10 – Processing of personal data relating to criminal convictions and offences

Article 10 of the GDPR restricts the processing of personal data concerning legal offences. Information about criminal convictions, offences or related security measures can be processed only pursuant to Union or national law, or under the control of an official authority. There are no other justifications. Even consent from the individual will not provide a justification under the Regulation to process this type of personal data.

Processing concerning legal offences

Article 10 of the GDPR precludes the banks from processing data relating to offences, criminal convictions or security measures.

(1) Bank customers

For the reasons elaborated upon in Section 3, it is critically important for the banks to maintain relevant information to alert their lending officers to the risks of making new or further advances to individuals who clearly do not qualify for such new or additional lending. Therefore, the banks may retain, on a particular **customer** file, press cuttings/ other information relating to court proceedings / convictions against that customer and similar information on any other person (e.g. a debtor of the customer) where such information may affect the relationship between the bank and the customer. This on the basis of maintaining the recognised 'Know Your Customer' principle.

(2) Applicants for business

In so far as applicants for business are concerned, criminal record checks about an applicant for business are carried out as part and parcel of the due diligence exercise which banks are obliged to conduct in terms of Prevention of Money Laundering laws or any other law. The decision as to whether a record of such checks is to be retained depends on whether or not the bank decides to take the applicant on board as a client or not.

If the applicant becomes a client, it is imperative that the latter is informed of the data being retained about him or her. It is important that strict retention periods for such data are adhered to. In the case of information which is publicly available, the bank could link to the official source rather than create its own record.

If an applicant for business is refused by the bank, the bank may wish to keep an annotation of the fact in the eventuality that the same applicant seeks to re-apply. It is important that any black lists created by the bank are not retained for longer than necessary to fulfil the conduct of due diligence requirements. In the case of information which is publicly available in relation to any such applicant for business, the bank could link to the official source rather than create its own record. Banks can also retain a flagging to the effect that business was declined due to diligence findings without maintaining any additional records.

(3) Recruitment

In terms of Section 7.4 of the FIAU's Implementing Procedures on Anti-Money Laundering, banks shall ensure that they have in place appropriate procedures for due diligence when engaging employees. This would generally include obtaining professional references, confirming employment history and qualifications and requesting a recent police conduct certificate. Consequently, banks as employers are under obligation to process such data as required in terms of the Implementing Procedures. In order to prove that they have abided by such requirement, banks are allowed to process and keep copies of police conduct certificates for selected candidates, given that such processing is deemed in compliance with Article 6 (1) (c) of the GDPR as discussed in Section 3. That said, given its sensitivity, such document shall be retained separately from other HR records which are accessed on a regular basis by HR personnel.

SECTION 7:

Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 13 – Information to be provided where personal data are collected from the data subject

Article 14 – Information to be provided where personal data have not been obtained from the data subject

The Regulation makes provision for the information which must be provided in privacy notices. It also requires controllers to ensure their privacy notices are "*concise, transparent, intelligible and easily accessible*" (Article 12 (1) of the GDPR).

The information which must be included in the privacy notice is the following:

- The identity and contact details of the controller and details of your representative (where applicable).
- The contact details of your data protection officer.
- The purpose and legal basis of processing. Where legitimate interests are relied upon, details of those interests.
- The right to withdraw consent (if this is the basis for such processing).
- The categories of personal data processed. This is only needed when personal data is obtained from a third party.
- The recipients or categories of recipients of personal data.
- The source of the personal data, including use of public sources. This is only needed when personal data is obtained from a third party.
- Details of any intended transfer outside the Union. Details of any safeguards relied upon and the means to obtain copies of transfer agreements.
- The period for which data will be stored or the criteria used to determine this period.
- A list of the individual's rights as per Article 13 (2) (b) and Article 14 (2) (c) namely, the right to request from the controller 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 .
- Details of any automated decision making, including details of the logic used and potential consequences for the individual.
- Whether provision of personal data is a statutory or contractual requirement, whether disclosure is mandatory and the consequence of not disclosing personal data. This is only needed when collecting personal data directly from the individual.
- The right to complain to a supervisory authority.

A privacy notice must be supplied to data subjects at the time they provide you with their personal data. If you obtain that personal data from or disclose it to a third party, the notice must be provided:

- within a reasonable time after obtaining the data, but at the latest within a month;

- if the personal data is used to communicate with the individual, at the latest when that communication is made; and

- if the personal data is disclosed to a third party, at the latest when that data is disclosed.

If you obtain that personal data from a third party, there is no need to provide a privacy notice if:

- the data subject already has the information;

- providing the information would be impossible or involve disproportionate effort, particularly where the processing is for archiving, scientific or historical research purposes or statistical purposes;

- the obtaining or disclosure is pursuant to Union or Member State law and there are appropriate measures to protect the data subject; or

- the information is subject to professional secrecy.

Finally, if you process that personal data for a new purpose, you must give prior notification to the data subject.

Article 12 (1) - Information to data subject

Banks must have in place a general privacy policy covering all types of data processing. They should also have internal privacy policies dealing with the processing of specific types of personal data, for instance, on cctv recordings, telephone recordings and also the monitoring of email and internet usage of staff members. Apart from information within the meaning of Article 13, such policies should provide detailed information the modalities concerning the intended usage of such data, including the situations where the bank may resort to such systems (e.g. review the CCTV recordings, or conduct specific monitoring concerning email or internet usage).

Article 14 – Data Collected from other sources

It is normal for banks in the course of their business, to require references from third parties on individuals who may be existing or prospective account holders, borrowers, guarantors, etc. Such references are collected from third parties, including Credit Reference Agencies, other banks, other existing customers and professional persons. Furthermore, banks may request additional documentation from third parties such as professional references in order to screen prospective employees as required under the FIAU Implementing Procedures, or to fulfil obligations emanating from other laws or for any other purpose.

In all such cases, since the necessary information is being sourced by the bank from a third party, the bank is obliged in terms of Article 14 of the GDPR to inform the potential customer/employee of the fact that the bank is sourcing such information from a third party and this upon first contact with the individual concerned. Within the context of the specific

scenarios described in the first paragraph above, the individual must therefore be so informed upon applying for a particular facility or the opening of an account or upon applying for a specific post with the bank.

SECTION 8: Article 15 – Right of access by the data subject

Individuals have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, a copy of the personal data and the following information:

- The purposes of the processing: The individual should have the right to verify the lawfulness of the processing the bank is carrying out;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer (see Section 23);
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with a supervisory authority;
- Where the personal data are not collected from the data subject, any available information as to their source;
- The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Whereas the controller must respond to the subject access request for free, a fee may be charged if the individual asks for further copies of the personal data. The bank may also refuse to respond to the request if it is manifestly unfounded or excessive (or charge an administrative fee). Where large volumes of personal data are processed, the individual should specify exactly what information or processing the request relates to.

It must be possible to make requests electronically. Where such a request is made, the information should also be provided electronically, unless otherwise requested by the individual.

The controller is entitled to withhold personal data if disclosure would "*adversely affect the rights and freedoms of others*" (Article 15 (4)).

With reference to the time for compliance in order to fulfil requests in relation to this right, the right to reject any such request, or the right to impose a fee, reference should be made to Section 15.

Article 15 – Right of access

1. Upon the request of a data subject, banks are obliged to provide to him/her not only "*confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and*" certain "*information*", but banks must also "*provide a copy of the personal data undergoing processing*". Strict timelines as defined in Section 15 of these Guidelines must be adhered to.

2. In response to such requests, banks may not be aware of particular information that is stored in files not pertaining directly to the person making the enquiry e.g. deceased customers' files containing details of the heirs, corporate client files containing details of individual shareholders and directors, etc. . In such cases banks are not to be expected to include such information in their response.

3. Any personal data relating to third parties and contained in the file of a customer making a request should not be included in a reply to an access request unless the bank has obtained the consent of such third party.

However in the case of a joint account, all parties to the account may have access to information relating to transactions passed over that account, notwithstanding that some or all of the transactions may have been originated by another joint account holder.

4. Article 15 (1) (h) of the GDPR requires banks responding to such requests to provide information about "*the existence of automated decision-making, including profiling, ... and, ..., meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*".

In this regard, no specific technical details or trade secrets should be divulged by the banks, though the logical sequence of such processing would need to be explained.

5. Banks must accede to requests by data subjects to access CCTV recordings in which they feature. This is so provided that such access does prejudice an ongoing criminal investigation. It is also important to note that the identity of any third parties who feature in such recordings must be masked or blurred.

SECTION 9: Article 16 – Right to rectification

Data subjects may request controllers to rectify personal data that has not been processed in accordance with the GDPR, in particular because of the incomplete or inaccurate nature of the data. The controller shall immediately rectify or complete the data accordingly and notify any third parties to whom data had been disclosed about the measures undertaken.

With reference to the time for compliance in order to fulfil requests in relation to this right, the right to reject any such request, or the right to impose a fee, reference should be made to Section 15.

SECTION 10: Article 17 – Right to erasure ("right to be forgotten")

The data subject has the right to obtain from the controller the erasure of personal data concerning him or her. The bank must comply with the request where:

- the individual has **objected** to the processing (other than in relation to objections to direct marketing) and there are no overriding legitimate grounds to justify that processing;
- the personal data is no longer needed for the purpose for which it was collected or processed;
- the individual withdraws consent and there are no other grounds for the processing;
- the personal data is unlawfully processed;
- there is a legal obligation under Union or Member State law to erase the personal data.

In all such cases, the controller must without undue delay erase the personal data processed both manually and by electronic means. If he had made the personal data public, he must take reasonable steps to inform other controllers of the request for erasure.

The controller **does not need to comply** with such a request if the processing is necessary:

- for exercising rights of freedom of expression or information;
- for compliance with a legal obligation under Union or Member State law;
- in the public interest or carried out by an official authority;
- for public interest in the area of public health;
- for archiving or research; or
- for legal claims.

With reference to the time for compliance in order to fulfil requests in relation to this right, the right to reject any such request, or the right to impose a fee, reference should be made to Section 15.

SECTION 11: Article 18 – Right to restriction of processing

The data subject has the right to obtain from the controller restriction of processing. You must comply with the request where:

- the individual has **objected** to the processing and you are considering if there are overriding legitimate grounds that justify continued processing;
- the processing is no longer necessary but retention of the data is needed by the data subject to deal with legal claims;
- the processing is unlawful but the individual wants the data to be restricted not erased; or
- the accuracy of the personal data is being contested and the controller is verifying that data.

Where data is restricted, you may only **process** personal data:

- with consent of the data subject;
- for legal claims;
- for protection of the rights and freedoms of others; or
- for reasons of important public interest.

The data subject shall be informed by the controller before the restriction of processing is lifted.

Controllers need to ensure that their systems are set up to identify restricted personal data and to limit access to that data.

With reference to the time for compliance in order to fulfil requests in relation to this right, the right to reject any such request, or the right to impose a fee, reference should be made to Section 15.

SECTION 12: Article 20 – Right to data portability

Individuals already have a right to access their personal data through a subject access request (see Section 8). Data portability enhances this right, giving the individual the right to get that personal data in a structured, commonly used and machine readable format. Individuals can also ask for the data to be transferred directly from one controller to another, where technically feasible (Article 20 (2)). There is no right to charge fees for this service.

However, this right:

- **only applies where the controller is processing personal data in reliance on the processing conditions of consent or performance of a contract.**

- **only applies if the data processing is carried out by automated means and therefore does not cover paper files.**

- **only applies to personal data concerning data subject.**

  You can only exercise the right to data portability with regard to personal data. Therefore, any data, which is anonymous or does not concern the data subject, cannot be requested. However, a data subject may request portability of pseudonymous data that can be clearly linked to the data subject (e.g. by him or her providing the respective identifier – Article 11 (2)).

- **only applies to personal data "provided to" the controller.**

  There are many examples of personal data which will be knowingly and actively "provided by" the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, **the data controller must also include the personal data that are generated by and collected from the activities of users in response to a data portability request, that is,** raw data. This latter category of data does not include data that are exclusively generated by the data controller, such as a user profile created by analysis of the raw data collected.

A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as "provided by the data subject":

- **Data actively and knowingly provided by the data subject are included** in the scope of the right to data portability (for example, mailing address, user name, age, etc.);

- **Observed data are "provided" by the data subject by virtue of the use of the service or the device**. They may for example include a person's search history. It may also include other raw data.

In contrast, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". These personal data do not fall within the scope of the right to data portability. For example, a credit score is a typical example of inferred data. Even though such data may be part of a profile kept by a data controller and are inferred or

derived from the analysis of data provided by the data subject, this data will typically not be considered as "provided by the data subject" and thus will not be within scope of the data portability right.

Nevertheless, the data subject can still exercise his or her *"right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data*" as well as information about "*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*". (Article 15 refers).

The term "provided by the data subject" must be interpreted broadly, and only to exclude "inferred data" and "derived data", which include personal data that are generated by a service provider (for example, algorithmic results). **A data controller can exclude those inferred data but should include all other personal data provided by the data subject** through technical means provided by the controller. This includes all data observed about the data subject during the activities for the purpose of which the data are collected, such as a transaction history or access log. Data collected through the tracking and recording of the data subject (such as technology used to track browsing behaviour) should also be considered as "provided by" him or her, even if the data are not actively or consciously transmitted.

Thus, the terms "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour but not subsequent analysis of that behaviour. By contrast, any personal data which have been generated by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.

- **The right to data portability must not adversely affect the rights and freedoms of others.**

This condition intends to avoid retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller in cases where these data are likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects (Article 20(4) of the GDPR). Such an adverse effect would occur, for instance, if the transmission of data from one data controller to another, under the right to data portability, would prevent third parties from exercising their rights as data subjects under the GDPR (such as the rights to information, access, etc.).

The data subject initiating the transmission of his or her data to another data controller either gives consent to the new data controller for processing or enters into a contract with them. Where personal data of third parties are included in the data set, another ground for lawfulness of processing must be identified. For example, a legitimate interest under Article 6(1)(f) may be pursued by the data controller to whom the data is transmitted, in particular when the purpose of the data controller is to provide a service to the data subject that allows the latter to process personal data for a purely personal or household activity.

For example, when a data subject exercises his/her right to data portability on his/her bank account, such an account can contain personal data relating to the purchases and

transactions of the account holder but also information relating to transactions, which have been "provided by" other individuals who have transferred money to the account holder. In this context, the rights and freedoms of the third parties are unlikely to be adversely affected in the webmail transmission or the bank account history transmission, if their data are used for the same purpose in each processing, i.e. as a contact address only used by the data subject, or as a history of one of the data subject's bank account. Conversely, their rights and freedoms will not be respected if the new data controller uses the contact directory for marketing purposes.

Therefore, to prevent adverse effects on the third parties involved, the processing of such a directory by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs. A receiving 'new' data controller (to whom the data can be transmitted at the request of the user) may not use the transmitted third party data for his own purposes e.g. to propose marketing products and services to those other data subjects. Otherwise, such processing is likely to be unlawful and unfair, especially if the third parties concerned are not informed and cannot exercise their rights as data subjects.

To further help reduce the risks for other data subjects whose personal data may be ported, all data controllers (both the 'sending' and the 'receiving' parties) should implement tools to enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data. Additionally, they should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. because they as well want to move their data to some other data controller. Such a situation might arise with social networks.

Data controllers must clearly explain the difference between the types of data that a data subject can receive using the portability right or the access right. It is also recommended that data controllers always include information about the right to data portability before any account closure. This allows users to take stock of their personal data, and to easily transmit the data to their own device or to another provider before a contract is terminated. As a best practice for "receiving" data, controllers ought to provide data subjects with complete information about the nature of personal data which are relevant for the performance of their services. This allows users to limit the risks for third parties, and also any other unnecessary duplication of personal data even where no other data subjects are involved.

With reference to the time for compliance in order to fulfil requests in relation to this right, the right to reject any such request, or the right to impose a fee, reference should be made to Section 15.

For guidance on the following questions, refer to attached Annex III to these guidelines:

- ***How can the data controller identify the data subject before answering his request?***
- ***What is the expected data format?***
- ***How do you deal with a large or complex personal data collection?***
- ***How can portable data be secured?***

- ***How do you help users in securing the storage of their personal data in their own systems***?

SECTION 13: Article 21 – Right to object

When the processing is legitimised on the basis of the controller's legitimate interests or based on the necessity of performing a task in the public interest, the data subject has the right to object at any time to the processing of his/her personal data, including any profiling. The controller shall no longer process the personal data unless the controller can demonstrate compelling legitimate grounds for such processing which override the interests, rights and freedoms of the data subject, or in order for the establishment to exercise or defend legal claims.

Right to object to direct marketing

The Regulation provides that individuals have the right to object to direct marketing (Article 21 (2) and (3)). When an individual exercises this right, the bank must not only stop sending direct marketing material to the individual, but also stop any processing of that individual's personal data for marketing purposes. For example, in the case of an objection from a data subject, the bank should stop profiling that individual for the purposes of direct marketing.

The e-Privacy Directive 2002/58EC, transposed under the local statute by virtue of Subsidiary Legislation 440.01, contains specific obligations for direct marketing by electronic means, and in principle, requires the prior consent of the individual. The e-Privacy Directive is still applicable.

With reference to the time for compliance in order to fulfil requests in relation to this right, the right to reject any such request, or the right to impose a fee, reference should be made to Section 15.

Article 21 (2) and (3) – Direct marketing

Communication for direct marketing purposes by means of an automatic calling machine, a facsimile machine or electronic mail are regulated by Subsidiary Legislation 440.01, and are hereunder referred to as '*communication by electronic means*'. SMS adverts and other forms of electronic messaging including instant messages (e.g. via social media or other similar platforms) are also considered as electronic mail for the purposes of such regulation. All other types of communications for direct marketing purposes are referred to as '*conventional mail*'.

Communication for direct marketing purposes of **third party products or services** (that is, products or services offered by a separate legal entity other than the bank itself which is conducting the advertising) via any medium whatsoever, (that is, whether via conventional mail, by electronic means or printed on any type of stationery issued by banks) always requires the explicit consent of the customer.

1) Conventional Mail

The processing of legitimately collected personal data for direct marketing purposes is allowed as long as the data subject does not give notice to the controller that he opposes it.

The controller is duty bound to appropriately inform the data subject of his right to oppose, at no cost, the processing for direct marketing purposes.

The provisions of Article 13 (2) (b) of the GDPR require that information about the right to oppose is appropriately given by the bank to its customers. In practice, this is normally done at the beginning of a relationship.

If no objection has been/ is received, banks may continue to process these customers' data for direct marketing purposes by conventional mail.

2) Communication by Electronic Means

Regulation 9 (1) of Subsidiary Legislation 440.01 prohibits the use of an automatic calling machine, or a facsimile machine, or electronic mail to make an unsolicited communication to a subscriber (whether a natural person or a legal person) for the purpose of direct marketing, **unless that subscriber has given his prior consent in writing to the receipt of such a communication**.

However, Regulation 9 (2) of Subsidiary Legislation 440.01 allows some leeway in this regard, in that where a customer's contact details for electronic mail have been obtained by a bank '*…in relation to the sale of a product or service'*, that bank may use such contact details '*…for direct marketing of its own similar products or services*.' But this leeway comes with a Proviso: '*That customers shall be given the opportunity to object … to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use'.*

3) Marketing material with stationery issued by banks

Stationery issued by banks, such as bank account statements, ATM receipts, transaction vouchers etc. may contain general additional information about the services offered by the bank or that of a third party. This information is not considered equivalent to direct marketing, provided that such communication is general in nature and not specifically tailored or targeted to a customer or group of customers based on their profile. By way of example, leaflets, circulars, inserts, accompanying Bank's stationery, but which are sent indiscriminately and which are not specifically addressed to an individual, would in principle, fall outside the scope of direct marketing. The same applies to information or advertising messages which are printed on the bank's stationery material, provided that there is no evidence to suggest that these messages are specifically targeted to the recipient.

SECTION 14:

Article 22 – Automated individual decision–making, including profiling

Individuals have the right not to be subject to decisions based solely on automated processing that produce legal effects or significantly affect the individual (Article 22). However, this right does not apply where the decision is:

- based on explicit consent from the individual, subject to suitable safeguards, including a right for a human review of the decision;
- necessary for a contract with the individual, subject to suitable safeguards, including a right for a human review of the decision; or
- authorised by EU or national law.

Additional restrictions apply to automated decision making or profiling using special categories of personal data or when carried out on children.

With reference to the time for compliance in order to fulfil requests in relation to this right, the right to reject any such request, or the right to impose a fee, reference should be made to Section 15.

Article 22 – Decisions based on automated processing

This Article applies in particular to credit scoring. Where the outcome of such scoring results in a request for credit facilities being declined, the applicant is entitled to:

1. Request that the decision be reconsidered other than in a manner based solely on automated processing.
2. Obtain information from the bank about what has controlled the automated processing that resulted in the negative decision.

Such obligations would not apply in those cases where the decision is necessary for entering into, or the performance of, a contract between the controller and data subject, or if it is established by a law laying down suitable safeguards and measures to protect the subject.

In any case, banks would have an obligation under Article 13 or 14, to inform data subjects about the existence of automated decision-making, by providing meaningful information about the logic involved and the consequences envisaged for the data subject. The bank, however, is not obliged to reveal specific information about the algorithm involved or the computations leading to a credit score. No specific technical details or trade secrets need to be divulged.

SECTION 15:

Other provisions relating to the rights of data subjects under Articles 15 to 22

15.1: Time for compliance by the data controller in order to fulfil requests by data subjects:

Article 12 (3) provides that the data controller must comply with the exercise of all the captioned rights **"*without undue delay*" and in any case "*within one month of receipt of the request*"** or within a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request.

Data controllers who do not take action on any request of the data subject must indicate to the data subject "*the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy*", no later than one month after receiving the request.

Data controllers must respect the obligation to respond within the given terms, even if it concerns a refusal. In other words, the data controller cannot remain silent when it is asked to answer a request.

15.2: In which cases can a request be rejected or a fee be charged?

Article 12 (5) prohibits the data controller from charging a fee for "*any communication and any actions taken"* in fulfilment of the captioned rights of the data subject, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, "*in particular because of their repetitive character*". In the latter case, the controller can refuse to act on the request but bears the burden of proving the manifestly unfounded or excessive character of the request.

The overall cost of the processes to answer requests, such as data portability requests, should not be taken into account to determine the excessiveness of a request. The overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer requests.

SECTION 16: Article 25 – Data protection by design and by default

The Regulation makes specific provisions on the use of technical and organisational measures tailored to enhance the level of data protection compliance. When deploying systems, applications, products or services that rely on the processing of personal data to fulfil their tasks, banks should take into account the right to data protection and should encourage their IT department or IT service providers, including developers, to design products or services that contain technical measures which are data protection friendly, embedded in the design.

Such measures could consist inter alia of:

- Facilitating data controllers in creating and improving security measures;
- Data minimisation and pseudonymisation;
- Transparency both in relation to processing and the functions within an organisation;
- Default settings which limit the processing of personal data to what is strictly necessary;
- Features enabling data subjects to have more control on their personal data including its access and further usage;
- Measures protecting data subjects' rights;
- Strong access controls including audit trails and flagging systems;
- Data segregation mechanisms;
- Automated deletion or anonymisation of personal data upon expiry of the storage period.

Similar measures shall be taken into consideration when issuing tenders for such services and in any case, well before the product design.

SECTION 17: Article 28 – Processor (Outsourcing)

The GDPR impacts on all aspects of the processing relationship, from how to choose a processor, to what to include in the processing contract and how data is dealt with at the end of that arrangement. It also impacts heavily on the risks associated with processing personal data for both controllers and processors, which in turn affects the contractual risk allocation between those parties.

Choosing a processor

Under the GDPR controllers can only use processors "*providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of GDPR and ensures the protection of the rights of data subjects*."

This is much broader than the current requirements and means that controllers must carry out a broader due diligence exercise when selecting a processor. Controllers may therefore consider whether it is necessary, or good practice, to carry out a data protection impact assessment (DPIA) before entering into a major new processing arrangement.

Negotiating a processor contract

The GDPR requires that whenever processing is carried out on behalf of a controller by a third party, such parties must enter into a **written** agreement (including in electronic form). The said agreement must clearly abide by the below requirements:

Article	Requirement
28 (3)	Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular, that the processor will:
28(3) (a)	process only on documented instructions, including with regard to transfers of personal data to a third country or to an international organisation (unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);
28 (3) (b)	ensure those processing personal data are under a confidentiality obligation (contractual or statutory);
28 (3) (c)	take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate;
28 (3) (d)	only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors;
28 (3) (e)	assist the controller in responding to requests from individuals (data subjects) exercising their rights;
28 (3) (f)	assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);
28 (3) (g)	delete or return (at the controller's choice) all personal data at the end of the

	agreement (unless storage is required by EU/member state law);
28 (3) (h)	make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instructions infringe data protection law.

It is important to note that while processors have some direct obligations, controllers still have more extensive liability than processors under the GDPR. They remain liable for all damage caused by processing which infringes the GDPR, whereas processors are only liable under the GDPR when they breach processor specific provisions or act outside the controller's instructions. Controllers are often reliant on processors to enable them to fulfil their legal obligations. Despite the detailed nature of Article 28(3), there are instances where banks, as controllers, may want to go beyond the GDPR's contractual requirements . For example, in relation to breach notification, controllers have an obligation to notify their supervisory authority of a data breach without undue delay and, where feasible, within 72 hours from the moment that they become aware of such breach. However, processors only have a duty to notify their controllers 'without undue delay'. In this regard, controllers should consider including specific terms in their contractual agreement with the processor, requiring them to notify the breach promptly and within an established timeframe, such as 24hrs.

In terms of Article 28 (7) and (8), both the European Commission and the supervisory authority may lay down standard contractual clauses for the matters alluded to above.

SECTION 18: Article 30 – Records of processing activities

Banks are no longer obliged to notify data processing activities to the Data Protection Commissioner. However, in view of the processing activities concerning regular and systematic monitoring of data subjects which are deemed to involve risks on the rights and freedoms of individuals, and also taking into account the processing of special categories of personal data, criminal convictions and offences, banks are subject to the record-keeping obligations emanating from Article 30.

Controllers:

If you act as a controller, you must keep a record of the following information:

- your name and contact details and, where applicable, any joint controllers, representatives and data protection officers;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients, including recipients in third countries or international organisations;
- details of transfers of personal data to third countries (where applicable);
- retention periods for different categories of personal data (where possible); and
- a general description of the security measures employed (where possible).

Processor

If you act as a data processor, you must keep the following records:

- your name and contact details and, where applicable, representatives and data protection officers;
- the name and contact details of each controller you act for including, where applicable, representatives and data protection officers;
- the categories of processing carried out on behalf of each controller;
- details of transfers of personal data to third countries (where applicable);
- a general description of the security measures employed (where possible).

Data protection impact assessment

The Regulation makes a privacy impact assessment mandatory for any new project that is likely to create "high risks" for individuals. The process for carrying out this assessment is set out below:

- **Is the processing likely to be "high risk"?**

High risk processing includes:

- systematic and extensive profiling that produces legal effects or significantly affects individuals;
- processing special categories of personal data on a large scale; and
- systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV).

The supervisory authority may identify other processing as being "high risk".

If yes, you must carry out an assessment. Your data protection impact assessment must be documented and must contain the following information:

- a description of the processing, including its purposes and any legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to individuals; and
- the measures taken to address those risks.

You must seek advice from your data protection officer and may have to consult with affected individuals or their representatives

- **Is the processing still "high risk"?** Does the assessment indicate your processing is high risk in spite of measures taken to mitigate that risk?

If yes, you must consult your supervisory authority. The supervisory authority will consider if your processing is compatible with the Regulation.

The supervisory authority should respond within eight weeks, but can extend this period by a further six weeks if extra time is needed due to the complexity of the processing. These time periods are suspended during periods in which the supervisory authority is waiting for further information from the banks.

SECTION 19: Article 32 – Security of processing

The Regulation requires banks to keep personal data secure. They are to take appropriate technical and organisational measures to protect their systems. This broad obligation is supplemented by additional obligations to take the following steps, **where appropriate** (Article 32):

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of its information technology systems;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

SECTION 20:

Article 33 – Notification of a personal data breach to the supervisory authority

Article 34 – Communication of a personal data breach to the data subject

In terms of Articles 33 and 34 of the Regulation, controllers are obliged to notify the supervisory authority and, in some cases, individuals, of personal data breaches unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The Article 29 Working Party issued guidelines on Personal Data Breach Notification, which were adopted in October 2017 and revised on 6th February 2018.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is potentially very broad. It is not limited to loss of data and extends to unauthorised access or alteration. However, it only captures actual breaches and not suspected breaches.

Where a personal data breach occurs as a result of cross-border data processing, or where it will substantially affect data subjects in more than one EU jurisdiction, this will lead to the use of the one-stop-shop mechanism, as contemplated under Article 60 of the GDPR. This is relevant in the case of banks having multiple establishments across the EU.

Is the breach a "risk"?

You must consider if the personal data breach is likely to be a risk to individuals. There is a "risk" to individuals if processing could lead to physical, material or non-material damage. This includes profiling or processing that could lead to discrimination, identity theft, damage to reputation or reversal of pseudonymisation. It includes any processing of special categories of personal data or personal data of children or other vulnerable persons or processing that involves large amounts of personal data.

If NO, notification is not required. However, you must document the personal data breach.

If YES, you must notify the supervisory authority without undue delay and, where feasible, within 72 hours from when you become aware of the breach. That notification should contain specified details of the breach. If you cannot provide all of those details immediately, you can provide them in stages. In order to facilitate such notification, the Information and Data Protection Commissioner will make available a specific form on the website www.idpc.org.mt.

Is the breach "high risk"?

You must consider if the breach is a high risk for individuals. The breach will not be high risk if the data is encrypted or other protective measures are in place.

If NO, no further notification is required. The process is at an end.

If YES, you must inform the affected individuals**.** You must provide affected individuals with details of the personal data breach without undue delay (though there is no fixed deadline). If informing the affected individuals directly would involve disproportionate effort, you may be able to use an alternative means of public communication, e.g. newspaper adverts.

You must keep a record of all security breaches, regardless of whether they need to be notified to the supervisory authority.

In view of the above, banks need to:

- Consider setting up a central breach management unit to collate, review and notify breaches, where appropriate.

- Review and update their security measures in light of the increased security obligations in the Regulation.

SECTION 21: Article 35 – Data protection impact assessment

Article 35 – Data Protection Impact Assessment

The GDPR imposes a legal obligation on banks to conduct a data protection impact assessment for any processing that is likely to create "high risks" for customers (see Section 18). Bank activities which can be considered to involve high risk processing, include conducting due diligence and especially enhanced due diligence in relation to any potential or existing customer as well as profiling of clients. Profiling activities which may lead to decisions including those by automated means, which have significant effects on data subjects, such as for example credit scoring, are considered to create high risk and would require an impact assessment.

SECTION 22: Article 37 – Designation of the data protection officer

In terms of Article 37 (1) (b) of the Regulation, banks are obliged to appoint a data protection officer.

The role of the data protection officer

The data protection officer is responsible for monitoring compliance with the Regulation, providing information and advice, and liaising with the supervisory authority. The data protection officer:

- must report to the highest level of management within your business;
- must be able to operate independently and not be dismissed or penalised for performing his/her tasks; but
- can have other roles so long as they do not give rise to a conflict of interests (i.e. this does not have to be a full-time role).

SECTION 23:

Article 46 – Transfers subject to appropriate safeguards

Article 49 – Derogations for specific situations

A transfer of personal data to a third country or an international organisation may take place where the European Commission has decided that the third country or one or more specified sectors within that third country, or the international organisation in question, ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Otherwise, the GDPR prohibits the transfer of personal data outside the Union, unless certain conditions are met by the controller or processor. The safeguards which must be in place are any of the following:

- A legally binding and enforceable instrument between public authorities or bodies;
- Binding corporate rules approved by the competent supervisory authority;
- Standard data protection clauses adopted by either the European Commission or by a supervisory authority and approved by the Commission;
- An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards as regards data subjects' rights;
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards as regards data subjects' rights;
- Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country authorised by the competent supervisory authority;
- Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights and authorised by the competent authority.

Therefore, in line with the above:

i. It will be possible to transfer personal data to a person outside the Union where the importer and exporter enter into the so-called Model Contracts. It is possible to enter into multiparty Model Contracts, commonly known as intra-group agreements. The existing controller-controller and controller-processor Model Contracts will be grandfathered. Where standard clauses approved by the Commission are used, authorisation from a supervisory authority will no longer be required.

ii. Transfers to third countries are possible if the importer has signed up to suitable Codes of Conduct or obtained suitable Certification.

iii. Binding corporate rules (BCRs) are a set of binding obligations under which a group of undertakings commit to process personal data in accordance with the Regulation. BCRs have been put on a statutory footing and will be available to both controllers and processors.

Banks could therefore consider implementing a "structural" transfer solution (such as binding corporate rules or an intra-group agreement) as these provide a general justification for your transfers.

In the case of transfer authorisations issued by the Commissioner on the basis of adequate safeguards (e.g. model clauses) prior to the GDPR, such transfers shall remain valid until amended, replaced or repealed, as may be necessary by the Commissioner.

The GDPR makes provisions for a number of specific situations where a transfer can take place even in the absence of the safeguards discussed above (Article 49 (1)). The below however, shall be narrowly interpreted and used in exceptional circumstances.

- there is the explicit consent of the data subject;
- the transfer is necessary for the performance of a contract with the individual or in the individual's interest;
- necessary for important reasons of public interest. That public interest must be recognised under Union or Member State law;
- necessary for the establishment, exercise or defence of legal claims;
- necessary for the vital interests of an individual where the individual is unable to give consent; or
- the transfer is made from a public register.

The GDPR also introduces a new exemption for minor transfers which is only available in limited situations. It was intended to legitimise one-off or occasional transfers of personal data, for example where employees take their laptop with them on holiday or email a person who happens to be outside the Union. The requirements to invoke the minor transfer exemption are the following:

- No other justification could be used
- The transfer is not repetitive
- Only limited data subjects are affected
- Supervisory authority and data subjects are informed of the transfer
- The risks have been assessed and safeguards applied
- There is a compelling interest not overridden by the individuals' interests

Articles 44 to 50 – Transfer of data to a third country / Exemptions from the prohibition of the transfer of data to a third country

In so far as cross-border credit transfers via SWIFT are concerned, it is to be clarified that such transfers are effected upon the application of the ordering customer who, by signing the transfer order, is also implicitly giving his consent to the transfer of the personal data contained in the transfer order to the jurisdiction where recipient of such transfer is located. However, banks are to inform their customers that pursuant to an Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Program (TFTP), their personal data could be disclosed to the U. S. authorities. MBA members have agreed to use the following wording in order to notify bank customers:

"*Personal data in relation to transactions effected via SWIFT (Society for Worldwide Interbank Financial Telecommunication) may be required to be disclosed to the United*

States authorities in order to comply with legal requirements applicable in the United States for the prevention of crime and in accordance with the EU-US Terrorist Finance Tracking Program (TFTP) agreement".

Other bank activities which often require the transfer of data to third countries and hence need to comply with the legal requirements set out in this Section, include offshoring activities which may be intra-group initiatives or may involve the use of a third party service provider such as, for example, the use of cloud services.

In the absence of a decision by the EU Commission recognising the third country to which a transfer is envisaged as adequate in terms of the data protection regime, banks would need to ensure that the transfers are subject to adequate safeguards and guarantees which are essentially equivalent to those afforded by EU law. In this regard, adequacy instruments which are recognised by the EU Commission for such purposes (e.g. EU Standard Contractual Clauses or Binding Corporate Rules), shall be considered depending on their suitability for the type and nature of transfer.

SECTION 24: Article 48 – Transfers or disclosures not authorised by Union law

In terms of Article 48:

"*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer...*"

As such, banks should respond to such requests only if they are routed through the competent national authority.

Annex I

Malta Bankers' Association

Archival Material Retention Periods

Preamble: This document reflects, inter alia, the requirements of:

- Regulations 4(11) and 4(13) of the Cooperation with Other Jurisdictions on Tax Matters Regulations (S.L.123.127).
- Article 163 of the Companies Act, Cap. 386.
- Article 19 of the Income Tax Management Act, Cap. 372.
- Regulation 13 of the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L.373.01)
- Conduct of Business Rulebook Phase II

A copy of each of these enactments is attached to this document for easier reference.

1. **Scope:**

The scope of this document is to set out industry standards to be adopted by member banks regarding the retention periods to be applied by them in relation to all documentation / material which is sent for archiving.

To this end, the document outlines the respective retention periods applicable to the various categories of documents which are sent for archiving, the "trigger date" for the start of such retention periods, and the form (original / scanned / electronic) in which the various documents should be retained for archiving purposes.

2. Definitions:

2.1. **Account data** is defined as electronic data which relates to all aspects of an account, excluding transaction data. It is often referred to as static data since, unlike transaction data, it does not change that often. Examples of account data include a customer's Final Withholding Tax instructions, opening of account details, mailing addresses, and residence status. Account data would typically consist of alphanumeric characters.

2.2. **Account information** is similar to account data, but it can either take the form of a paper record, or alternatively, it can be a full scan of the document concerned. The difference between account data and account information is that the latter would

typically not be limited to alphanumeric inputs, but would include also signatures as well as pre-printed clauses. An opening of account form, be it original or scanned, would typically qualify as being account information. By contrast, the details of that form, as captured through a keyboard or similar device, would be called account data.

2.3. **Transaction data** is defined as electronic data which relates to the various debit or credit transactions that would pass through the account over the years. Examples of transaction data include the amount, details of payment, etc. Transaction data would typically consist of alphanumeric characters, and may cover all type of accounts, be they customer accounts or general ledger accounts.

2.4. **Transaction information** is similar to transaction data, but transaction information would typically reside on paper or is scanned. Compared with transaction data, transaction information would typically include the customer's signature as well as pre-printed clauses. A cheque or a voucher, be it original or scanned, would typically qualify as being transaction information. By contrast, the alphanumeric details of that cheque, as captured through an electronic device such as a keyboard, would then be called transaction data.

3. General points:

3.1. Each member bank is to adhere to the time period stipulated in this agreement.

3.2. Each member bank has the option to archive documents in paper and/or in scanned format, provided that the scan covers all the required information, including signatures and pre-printed clauses. There are four exceptions to this clause, namely:

3.2.1. ...cheques and other documents containing customers' signatures. Such documents must be held in their original paper format for a period of one year from date of presentation / creation of the document.

3.2.2. ...where the bank obtains documents certified by third parties (i.e. not being officers or employees of the subject person) in fulfilment of their obligations under the Implementing Procedures issued by the Financial Intelligence Analysis Unit. In such cases, banks should retain on file the physical document certified by the third party and not a copy thereof (Section 5.4 of the Implementing Procedures).

3.2.3. ...obsolete collateral (security) documents. Such documents should be retained in their original format, except where the bank is obliged to return the original document (e.g. guarantees issued in favour of the bank by another bank).

3.2.4. ...obsolete Powers of Attorney. Such documents should be retained in their original format.

3.3. The start date for the retention period shall vary from one case to another, as explained in section five of this document.

4. The various categories of retention periods:

4.1. All documentation which the bank is required to keep in terms of Article 163 of the Companies Act and / or Article 19 of the Income Tax Management Act, must be retained for a period of ten years, starting from the end of the relative financial year. This typically includes all the documentation which relates to the day-to-day administration of the bank, such as payroll, purchases, utility bills, travelling expenses, capital expenditure, etc. This provision also includes a requirement to hold, for ten years, a full set of audited accounts, supported by all relevant working papers and computer generated reports detailing interest paid and received, exchange revaluation workings, etc. Such information may be retained in paper and / or in scanned or electronic formats.

4.2. All transaction data (see definition) is to be retained for a period of ten years from the date of the transaction.

4.3. All account data (see definition) is to be retained for a period of ten years from the date of closure of the respective account.

4.4. In so far as the retention of records which pertain to the following categories, Member Banks shall distinguish between the different categories as follows:

4.4.1 **Telephone recordings**

The retention period for telephone recordings varies depending on the purpose for processing such recordings.

(i) Telephone recordings which are the only proof of a debit authority or of a contract including those telephone conversations relating to transactions concluded when dealing on own account, and the provision of client order services that relate to the reception, transmission and execution of client orders, will be retained for a period of ten years from date of recording.

(ii) In all other cases, telephone recordings ought not to be kept for a period longer than thirty days.

(iii) Banks can exercise their own discretion in so far as telephone recordings which are used for training purposes are concerned, provided that the recordings are edited to ensure that no personal data is revealed and the identity of the caller and as much as possible the voice of the same caller are rendered non-identifiable.

4.4.2 **Video recordings**

Video recordings should not be retained for a period longer than necessary.

(i) In so far as customer-facing footage is concerned, such period shall not be longer than 30 days, provided that where specific footage is used in connection with an investigation, a copy of the relevant extract from the recordings may be retained as evidence until the case is concluded.

(ii) Back-office operations footage does not as a rule capture the faces of the employees, but only their hands and the cash handling process. In such cases, the footage of back-office operations can be kept for a period which is not longer than 90 days.

4.4.3 **Staff records**

Staff records shall also be subject to pre-defined retention periods, based on the purpose of processing and subject to operational and legal requirements applicable to such data. In this regard, banks shall distinguish between personal data which relates to records being renewed periodically (e.g. attendance, vacation leave, sick leave records) and which therefore may be substituted by or updated with new records on an annual basis, and other information which will be necessary for the entire duration of the employment relationship (e.g. employment contract, payroll and other financial records, qualifications, training, performance records and appraisals).

In the case of attendance, sick leave and vacation leave records, banks should determine internal practices as to the period within which any concerns or disputes may be raised internally on such matters, unless there are additional time frames stipulated by law. In these instances, and unless specific disputes arise, a maximum retention period of one year is deemed sufficient.

With regards to other staff records which are deemed necessary throughout the entirety of the employment relationship, retention periods shall be established from the date when the employment contract is terminated. Financial records are subject to obligations emanating from the Income Tax Act, and therefore shall be retained for ten years following termination of employment. In the case of other employment records, banks shall take into consideration possible legal action or claims for damages that may arise after termination of employment (e.g. unfair dismissal, bullying, sexual harassment, occupational health and safety, injury at work). Taking into account the possible legal prescriptive periods, a maximum retention period of five years after termination is deemed sufficient.

The abovementioned retention periods are without prejudice and may be superseded by general guidelines or code of ethics issued in the field of HR and employment, as may be approved from time to time by the Commissioner.

4.4.5 **Internal documentation such as circulars, obsolete handbook procedures and documentation and communication records as exchanged with third parties other than with customers (such as with suppliers)**

The retention period for these categories, provided that there is no personal data, is left at the discretion of the bank.

4.5. Deceased customers' files are to be retained for a period of ten years from when the account balance was fully distributed to the heirs.

5. The "trigger date" for the start of the retention period:

5.1. The "trigger date" for transaction data, account data, deceased customers' files, and for other requirements as stipulated by the Companies Act and / or by article 19 of the Income Tax Management Act, have all been explained under section four above.

5.2. Transaction information (see definition) is typically held in paper format or as a full scan. Such records are to be held for a period of six years from date of transaction. Banks usually refer to this as the "daily waste". After six years, the bank may therefore destroy such paper records or scanned images. In so doing, the bank would then be relying on the corresponding transaction data (see definition) for a further four years, since transaction data must be retained for ten years (see paragraph 4.2 above).

5.3. Account information (see definition), is typically held in paper format or as a full scan. Such information is to be retained for a period of six years from the date when the account is closed. After six years, the bank may therefore destroy such paper records or scanned images. In so doing, the bank would then be relying on the corresponding account data (see definition) for a further four years, since account data must be retained for ten years (see paragraph 4.3 above).

5.4. Obsolete collateral (security) items must be retained for a period of six years from the date when the item was discharged.

5.5. Advances files must be retained for a period of six years, which shall start to run from the date when the respective facility has been closed (unless legal proceedings in respect of such repaid facilities are instituted during this period, in which case the relative files should be retained beyond six years until the conclusion of the legal proceedings).

Member banks, however, have no obligation to retain "old" advances files for more than thirty years after they were archived, even though credit facilities to the customer concerned have been ongoing.

This thirty year limit shall not apply to home loans, where the file must be retained for a period of six years from date of closure. Thus a file for a forty year home loan must be retained in its entirety for the full duration of the loan, plus a further six years.

"Classified Debt" files are to be treated in the same way as other advances files. If and when the debt is fully repaid, or a compromise is reached with the debtor whereby a lesser amount is accepted by the bank in full and final settlement of the debt, the file is to be retained for a period of six years from the date when the debt has been fully repaid, or the agreed settlement amount has been received. Otherwise, where the debt remains outstanding (irrespective of whether or not the debt has been written down / off in the bank's books), the file is to be retained for at least thirty years after it was archived.

5.6. Fact finds / Know Your Customer (KYC) records or similar investment-related reviews, portfolio management instructions, statements of compliance, etc. are to be retained for six years. The six years shall start to run after the end of the investment relationship.

Other documentation relating to the sale of investment to customers is to be retained for a period of six years from the date when the sale was concluded. In the case of documentation relating to life insurance products, such documentation is to be retained for the lifetime of the insured customer from the date when the sale was concluded and a period of six years thereafter.

5.7. The documentation which relates to all contracts, other than those mentioned elsewhere in this section, is to be retained for a period of six years which shall start to run from the date when such a contract is terminated or paid off or expired. Examples under this category include safe deposit lockers, guarantees issued by the bank, and letters of credit.

APPENDICES

A. Abridged version of the Archival Material Retention Period Document

B. Regulations 4(11) and 4(13) of the Cooperation with Other Jurisdictions on Tax Matters Regulations (S.L. 123.127).

C. Article 163 of the Companies Act, Cap. 386.

D. Article 19 of the Income Tax Management Act, Cap. 372.

E. Regulation 13 of the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01)

Appendix I: Summary of Retention Periods

Paragraph	Archival Material	Retention Periods
4.1	Documentation to be kept in terms of Article 163 of the Companies Act/ Article 19 of the Income Tax Management Act.	10 years, starting from the end of the relative financial year.
4.2	Transaction Data (See 2.3)	10 years from the date of the transaction.
4.3	Account Data (See 2.1)	10 years from the date of closure of the account.
4.4.1	Telephone Recordings	- 10 years from the date of recording if this is the only proof of a debit authority or of a contract. - Otherwise, maximum 30 days, but - If recordings are used for training purposes, retention period is at bank's discretion, provided recordings are suitably edited (see 4.4.1 (iii)).
4.4.2	Video Recordings	- Maximum 30 days for customer-facing footage (unless footage is required in connection with an ongoing investigation). - Maximum 90 days for back-office operations footage.
4.4.4	Staff Records: - Periodically reviewed records (e.g. attendance, vacation leave, sick leave) - Records kept for the entire duration of the employment relationship: - Payroll and other financial records - Other employment records	 - 1 year is deemed sufficient, unless specific disputes arise. - 10 years following termination of employment. - Maximum 5 years following termination of employment.
4.4.5	Internal Documentation	At bank's discretion, provided no personal data which is not public is contained therein.
4.5	Deceased Customers' Files	10 years from when the account balance was fully distributed to the heirs.
5.2	Transaction Information (See 2.4)	6 years from date of transaction.
5.3	Account Information (See 2.2)	6 years from the date when the account is closed.
5.4	Obsolete Collateral (Security) Item	6 years from the date when the item was discharged.
5.5	Advances Files (Including "Classified Debt" files)	6 years from the date when the facility has been closed (unless legal proceedings are in train).

		Note: "Old" advances files, other than files relating to home loans, need not be retained for more than 30 years, even if facilities to the customer concerned have been ongoing.
5.6	Investment Services: - Fact finds, KYC records or similar investment- related reviews, portfolio management instructions, statements of compliance, etc. - Other documentation related to the sale of investment products	- 6 years after the end of the investment relationship. - 6 years from the date when the sale was concluded.
5.7	Documentation related to the sale of life insurance products	To be retained for the duration of the policy plus a period of six years thereafter.
5.8	Documentation related to all other contracts (e.g. safe deposit lockers, guarantees issued by the banks, letters of credit, etc.)	6 years from the date when the contract is terminated, paid off or expired.

Appendix II

Aim of these regulations. *Substituted by: L.N. 384 of 2015.*

3. These regulations shall apply in order to ensure the effective cooperation with other jurisdictions on tax matters where arrangements that enable such cooperation are in place and shall be interpreted accordingly. Such cooperation shall include the exchange of information relating to a group request.

Availability of ownership information. *Amended by: L.N. 472 of 2012; L.N. 344 of 2017.*

4. (1) Entities shall keep updated information that identifies their owners and the level and type of their respective ownership stakes in such entities, including information on legal and beneficial owners. Such information is to be updated and documented not later than fourteen days from the date that the entity was notified or from the date the entity becomes aware of there being a new owner or of any change relating to existing owners. For the purposes of these regulations, "owners" include -

(*a*) in the case of a company, partnership and other any other body of persons (other than a foundation), the legal owners; and

(*b*) in the case of a foundation, the founders, the administrators, the members of the supervisory council, and the beneficiaries (where applicable), as well as any other person with the authority to represent the foundation.

(2) The provisions of sub-regulation (1) do not apply to -

(*a*) a publicly-traded company: provided that in the case of a publicly-traded company that is either resident in Malta or created under Maltese law, the required ownership information in relation to such companies is to be kept either by the company itself or by a central securities depository resident in Malta. For the purposes of this paragraph, "central securities depository" has the meaning found in article 2 of the Financial Markets Act; and

Cap. 345.

(*b*) public collective investment schemes.

(3) For the purposes of these regulations -

(*a*) where in any instance within an ownership chain, the legal owner acts on behalf of any other person as a trustee, fiduciary (including nominee) or under a similar arrangement, such a legal owner shall have the obligation to keep the information that identifies such other person;

(*b*) a company that has issued share warrants in accordance with article 121 of the Companies Act shall inform the competent authority in Malta of such issue not later than one month from the date of publication of these regulations in the case of share warrants issued before the said date, or fourteen days after the date of any issue made after the said date. Such companies shall also keep a register with the information that identifies the owners of such share warrants. Notwithstanding any other provision in any Act, a person in possession of a share warrant shall not

Cap. 386.

be entitled to any rights in relation to such share warrant unless the relevant company has been provided with the information that identifies such person. Furthermore, notwithstanding any other provision in any Act, a transfer of such share warrant shall not be valid at law if the relevant company has not been informed within fourteen days of the said transfer of the information that identifies the new owner:

Provided that the provisions of the preceding paragraph shall have effect up to 27 December 2017.

(4) (*a*) Trustees that are established under the laws of Malta or that are resident in Malta shall take all reasonable measures to ensure that updated information is kept that identifies the settlor, other trustees, the protector (if any) and beneficiaries of express trusts (whether the proper law of such trusts is that of Malta or elsewhere).

(*b*) Persons that are established under the laws of Malta or that are resident in Malta and that are entrusted with the administration of express trusts (whether the proper law of such trusts is that of Malta or elsewhere) shall have the same obligations as those found under paragraph (*a*).

(5) Information that identifies a person includes -

(*a*) in the case of an individual:

(i) the full name and surname;

(ii) the passport number, ID number or tax identification number;

(iii) date and place of birth if no number referred to in sub-paragraph (ii) is available; and

(iv) address of residence;

(*b*) in the case of persons that are not individuals:

(i) name;

(ii) date of inception or incorporation; and

(iii) registered address.

(6) Information that identifies a person is to be kept in Malta. However, such records may be kept in a jurisdiction with which Malta has an arrangement, that would permit exchange of ownership information.

Availability of accounting information.

(7) Individuals (engaged in a trade, business, profession or vocation), entities and trustees are to ensure that reliable books of account are kept that -

(*a*) correctly explain all transactions of such individual, entity or trust;

(*b*) enable the financial position of such individual, entity or trust to be determined with reasonable accuracy at any time; and

(*c*) allow financial statements to be prepared.

(8) Apart from the books of account referred to in sub-regulation (7) records to be kept shall further include underlying documentation, such as invoices, contracts, etc. and should reflect details of -

(*a*) all sums of money received and expended and the matters in respect of which the receipt and expenditure takes place;

(*b*) all sales and purchases and other transactions; and

(*c*) the assets and liabilities of the relevant individual, entity or trust.

(9) In the case of a company that is considered to be an entity for the purposes of these regulations, the financial statements are to be prepared and audited as required under the Companies Act or the Co-operatives Act, as the case may be.

Cap. 386.
Cap. 442.

(10) Accounting records are to be kept in Malta. However, such records may be kept in a jurisdiction with which Malta has an arrangement that would permit exchange of information of such records.

Availability of banking information.

(11) Banks that are considered to be entities for the purposes of these regulations are to ensure that banking information is kept on all account-holders in relation to their banking activity in Malta. For the purposes of these regulations, "banking information" includes all records pertaining to the accounts as well as to related financial and transactional information.

Prompt transmission of information.

(12) The information that is required to be kept in accordance with this regulation shall be kept in such a way that it may be submitted without difficulty to the Commissioner following a request made pursuant to the provisions of article 10A of the Income Tax Management Act. Where, following representations made by the requested person, the Commissioner is satisfied that for reasons that are beyond the control of such requested person, information cannot be submitted within the time limit specified in the original request made by the Commissioner to such requested person, the Commissioner shall consider allowing such other time limit as may be reasonable for the particular case In such cases, the provisions of regulation 6(1) and (2) shall apply taking into consideration such other time limit that is determined by the Commissioner.

Cap. 372.

Retention period.
Cap. 372.

(13) Subject to the provisions of article 19 of the Income Tax Management Act, entities, trustees and other persons that are required to keep information, records or documents under any of the provisions of this regulation shall keep such information, records and documents for a minimum period of five years from the end of the year in which the relevant transactions, acts or operations took place (including where the relevant entity or trust is liquidated or is no longer in existence). This requirement shall also apply to any person referred to in regulation 5(1) acting in a professional capacity in relation to any such information or records that he holds in the carrying on of his business.

Appendix III

court shall notify the auditor of the application and shall hear both parties before making a decision on the company's application.

(5) Unless the auditor receives notice of such an application before the end of the period of twenty-one days beginning with the day on which he deposited the statement, he shall within a further seven days send a copy of the statement to the Registrar.

(6) If the court is satisfied that the auditor is using the statement to secure needless publicity for defamatory matter -

(*a*) it shall direct that copies of the statement need not be sent out; and

(*b*) it may further order the company's costs on the application to be paid in whole or in part by the auditor, notwithstanding that he is not a party to the application;

and the company shall within fourteen days of the court's decision send to the persons mentioned in sub-article (3)(*a*) a statement setting out the effect of the order.

(7) If the court is not so satisfied, the company shall within fourteen days of the court's decision -

(*a*) send copies of the statement to the persons mentioned in sub-article (3)(*a*); and

(*b*) notify the auditor of the court's decision,

and the auditor shall within seven days of receiving such notice send a copy of the statement to the Registrar.

Failure to comply with article 161.

162. (1) If a person ceasing to hold office as auditor fails without just cause to comply with the provisions of article 161 he shall be liable to a penalty.

(2) In proceedings for a default under sub-article (1) it shall be a defence for the person against whom action is taken to show that he took all reasonable steps and exercised all due diligence to avoid that default.

(3) If a company makes default in complying with the provisions of article 161, every officer of the company who is in default shall be liable to a penalty, and, for every day during which the default continues, to a further penalty.

Chapter X - Accounts, Audit and Annual Return

Keeping of accounting records. *Amended by: L.N. 425 of 2007.* Cap. 13.

163. (1) In lieu of the requirements of articles 13 to 18 of the Commercial Code a company shall be required to keep proper accounting records with respect to -

(*a*) all sums of money received and expended by the company and the matters in respect of which the receipt and expenditure takes place;

(*b*) the assets and liabilities of the company;

(*c*) if the company's business involves dealing in goods:

(i) statements of stocks held by the company at the end of each accounting period of the company;

(ii) all statements of stocktakings from which any such statement of stocks as is mentioned in sub-paragraph (i) has been or is to be prepared; and

(iii) except in the case of goods sold by way of ordinary retail trade, statements of all goods sold and purchased, showing the goods and the buyers and sellers in sufficient detail to enable all these to be identified.

(2) For the purposes of sub-article (1), proper accounting records shall be deemed to have been kept with respect to the matters aforesaid if such records are sufficient to show and explain the company's transactions and are such as to -

(*a*) disclose with reasonable accuracy, at any time, the financial position of the company at that time; and

(*b*) enable the directors to ensure that any balance sheet and profit and loss account prepared under this Chapter complies with the requirements of this Act.

(3) The accounting records shall be kept at the registered office of the company or at such other place as the directors think fit, and shall be at all times open to inspection by the officers of the company:

Provided that if accounting records are kept at a place outside Malta there shall be sent to, and kept at a place in Malta and at all times be open to the inspection of the officers of the company such accounts and returns with respect to the business dealt with in the accounting records so kept as will disclose with reasonable accuracy the financial position of that business at intervals not exceeding six months and will enable to be prepared, in accordance with this Act, the company's balance sheet and its profit and loss account.

(4) A parent company which has a subsidiary undertaking, in relation to which the above requirements do not apply, shall take reasonable steps to secure that the subsidiary undertaking keeps such accounting records as to enable the directors of the parent company to ensure that any balance sheet and profit and loss account prepared complies with the requirements of this Act.

(5) Notwithstanding the provisions of article 26 of the Commercial Code, the accounting records of the company shall be kept for a period of ten years: Cap. 13.

Provided that where the accounting records are kept in a bound or unified form, the ten years shall commence to run from the date of the last entry made therein.

(6) If a company fails to comply with any provision of sub-articles (1) to (4), every officer of the company who is in default shall be guilty of an offence and liable on conviction to a fine (*multa*) of not more than eleven thousand and six hundred and

forty-six euro and eighty-seven cents (11,646.87), unless he shows that he acted diligently and that, in the circumstances in which the company's business was carried on, the default was excusable.

(7) If a company fails to comply with the provisions of sub-article (5), every officer of the company who is in default shall be liable to a penalty.

Accounting reference period and accounting reference date.

164. (1) A company's accounting periods are determined by reference to its accounting reference date.

(2) A company may give notice in the prescribed form to the Registrar specifying a date in the calendar year as being its accounting reference date:

Provided that no such notice shall have effect unless it is given before the end of nine months beginning with the date of the company's registration; and, failing such notice, the company's accounting reference date shall be the thirty-first of December.

(3) A company's first accounting reference period shall be such period ending with its accounting reference date as begins on the date of its registration and is a period of not less than six months and not more than eighteen months; and each successive period of twelve months beginning after the end of the first accounting reference period and ending with the accounting reference date shall also be an accounting reference period of the company.

(4) A company's first accounting period shall commence on the first day of its first accounting reference period and shall end on a date not more than seven days before or after the end of that accounting reference period as the directors may determine. Subsequent accounting periods shall commence on the day immediately following the company's previous accounting period and shall end on a date not more than seven days before or after the end of the next accounting reference period as the directors may determine.

(5) The directors of a parent company shall secure that, except where there are good reasons against it, the accounting period of each of its subsidiary undertakings shall coincide with the parent company's own accounting period.

Alteration of accounting reference period. *Amended by: IV. 2003.70.*

165. (1) At any time during a period which is an accounting reference period of a company by virtue of article 164 or 166 the company may give notice in the prescribed form to the Registrar specifying a date in the calendar year ("the new accounting reference date") on which that accounting reference period ("the current accounting reference period") and each subsequent accounting reference period of the company is to be treated as coming to an end or, as the case may require, as having come to an end.

(2) At any time after the end of a period which was an accounting reference period of a company by virtue of article 164 or 166 the company may give notice in the prescribed form to the Registrar specifying a date in the calendar year ("the new accounting reference date") on which that accounting reference

Appendix IV

or to give such information, particulars or evidence as may be required in replacement.

(2) Nothing in this article contained shall affect the provisions of article 30(4) and (5) or article 31(5) and (6), nor shall the Commissioner be empowered to require a copy of any return, statement or form, or the provision of any information, particulars or evidence in respect of any year of assessment where the raising of the relative assessment is statute-barred in terms of the provisions of the said subarticles.

Records to be kept. *Amended by: XX.1996.21; II. 2007.23; IV. 2007.26.*

19. (1) Every person carrying on a trade, business, profession or vocation shall keep proper and sufficient records of his income and expenditure to enable his income and allowable deductions to be readily ascertained.

(2) The records referred to in subarticle (1) shall include:

(*a*) proper accounts with respect to -

(i) all sums of money received or expended and the matters in respect of which the receipt or expenditure takes place; and

(ii) all sales, purchases or services rendered, as well as any other transaction, act or operation pertaining to the trade, business, profession or vocation;

(*b*) a profit and loss account or equivalent annual statement;

(*c*) a statement of the assets and liabilities as on the date on which the annual accounts of the trade, business, profession or vocation are made up or, in the case of a company, a balance sheet.

(3) Subject to such conditions as he may deem fit to impose, the Commissioner may exempt any person in respect of any year of assessment from keeping any record or statement referred to in subarticle (2).

(4) The records required to be kept under the provisions of this article shall be supported by such documents as may be appropriate in the circumstances, including -

(*a*) in the case of a company registered in Malta, the balance sheet and profit and loss account, which shall comply in every respect with the applicable provisions of articles 167, 168 and 169 of the Companies Act and notwithstanding any exemption made by that Act or by any other law, such balance sheet and profit and loss account shall be accompanied by a report made out by a certified public auditor as provided by the applicable provisions of articles 179 and 181 of that Act: Cap. 386.

Provided that in the case of a company which is not resident in Malta, such records shall be those which refer to the company's activities in Malta:

Provided further that the auditor's report mentioned in

this paragraph shall not be required for the first two accounting periods of a newly registered company whose sole shareholders are graduates of a Post-Secondary Institution who have set up the new company within three years of graduating and subject to such conditions, including the amount of turnover, as may be prescribed.'

(*b*) in the case of a co-operative society, the audited financial statements of the society, prepared in all respects as required by the law for the time being in force regulating co-operative societies and accompanied by any report which is by any such law required to accompany the audited financial statements of the society.

(5) All records required to be kept by any of the provisions of this article shall be retained for a period of not less than nine years after the completion of the transactions, acts or operations to which they relate:

Provided that the provisions of this subarticle shall not apply where effect has been given to the provisions of article 26, of article 163(5) or of article 324(2) of the Companies Act.

Cap. 386.

Certain powers of the Commissioner. *Amended by: XI. 2001.31; II. 2005.33; L.N. 425 of 2007; IV. 2011.59.*

20. (1) The Commissioner, or any officer authorised by him in writing shall have full and free access to all business or professional premises such as offices, factories, workshops, warehouses, garages and land serving such purposes in order to inspect any books, documents, accounts, returns and electronic data or to observe and record the nature and importance of any business or professional activity carried on there, and to check the existence of merchandise and means of production and transport and shall have full and free access to any property or other asset whose value is required to be determined for any of the purposes of the Income Tax Acts to the extent that such access is likely to assist him in determining the said value:

Provided that the Commissioner or any officer authorised by him as aforesaid may not seize any notarial act or register, and may not inspect public wills, the acts of delivery of secret wills and registers thereof during the life of the testator or testators, without the permission in writing of such testator or testators:

Provided further that the Commissioner or any officer authorised by him as aforesaid may not inspect any document or other record which is protected by the duty of professional secrecy or listen to any conversation or recording device which is protected by the same duty.

(2) If, in the exercise of his powers under subarticle (1), the Commissioner or a person authorised by him as aforesaid, requires access to premises occupied in whole or in part for the purposes of habitation, such access shall require the presence of an officer of the Police of a rank not below that of inspector and shall not take place between nine in the evening and five in the morning.

Appendix V

persons or institutions established in a Member State subject to national provisions implementing Directive (EU) 2015/849 and which comply fully with group-wide policies and procedures equivalent to those mentioned under regulation 6.

(3) Subject persons relying on another subject person or a third party shall obtain from that other subject person or third party the information required in accordance with the provisions under regulation 7(1)(a) to (c).

(4) Subject persons relying on another subject person or a third party shall take adequate steps to ensure that, upon request, that other subject person or third party shall immediately forward to them relevant copies of the identification and verification data relevant to the customer and the beneficial owner and other relevant documentation required in terms of regulation 7(1)(a) to (c).

(5) Subject persons that are branches or majority owned subsidiaries of persons or institutions established in a Member State or a third country other than Malta and subject persons that have branches or majority owned subsidiaries in a Member State or a third country shall be considered to comply with the provisions of sub-regulations (2) to (4) through the group's policies and procedures, where all the following conditions are met:

(a) the subject person relies on information provided by a third party that is part of the same group;

(b) that group applies customer due diligence measures, record keeping measures and anti-money laundering and counter-funding of terrorism policies and procedures equivalent to those under these regulations;

(c) the effective implementation of the measures and requirements referred to in paragraph (b) at group level is subject to supervision by a relevant authority.

(6) This regulation shall not apply to outsourcing or agency relationships where, on the basis of a contractual agreement, the outsourcing service provider or agent is to be regarded as part of the subject person.

Record keeping procedures.

13. (1) Subject persons shall retain the following documents and information for the purposes of the prevention, detection, analysis and investigation of money laundering or funding of terrorism activities by the Financial Intelligence Analysis Unit, relevant supervisory authorities, or law enforcement agencies in accordance with the provisions of applicable law:

(a) in relation to any business relationship that is formed or an occasional transaction that is carried out, the

customer due diligence documentation, data and information obtained in fulfilment of the requirements under regulations 7 to 12;

(b) supporting evidence and records necessary to reconstruct all transactions carried out by that person in the course of a business relationship or any occasional transaction, which shall include original documents or other copies admissible in court proceedings;

(c) a record of any disclosures made to the Financial Intelligence Analysis Unit in accordance with regulation 15(3);

(d) a record of any internal reports made in accordance with regulation 15(1)(a);

(e) a record of any written determinations made in accordance with regulation 15(1)(b);

(f) a record of any training provided in accordance with regulation 5(5)(e); and

(g) any other document, data or information which the Financial Intelligence Analysis Unit may require to be maintained in accordance with procedures and guidance issued in terms of regulation 17.

(2) The documentation, data or information referred to in sub-regulation (1) shall be kept for a period of five years commencing on –

(a) in relation to the documentation, data or information described in paragraph (a), the date when the business relationship ends or when the occasional transaction is carried out, and where the formalities necessary to end a business relationship could not be observed, the date on which the last transaction in the course of that business relationship was carried out;

(b) in relation to the supporting evidence and records described in paragraph (b), the date when all dealings taking place in the course of the transaction in question were completed;

(c) in relation to the records described in paragraphs (c) to (e), the later between the following:

(i) the date when the business relationships ends or the occasional transaction is carried out; or

(ii) the date when the report or determination is submitted or drawn up, as the case may be;

(d) in relation to the records described in paragraph (f), the date when the event referred to therein took place:

Provided that, in relation to records relating to an occasional transaction consisting in several operations which appear to be linked, the aforesaid period of five years shall commence on the date on which the last operation took place:

Provided further that, the period of five years may be further extended, up to a maximum retention period of ten years, where such extension would be considered necessary for the purposes of the prevention, detection, analysis and investigation of money laundering or funding of terrorism activities by the Financial Intelligence Analysis Unit, relevant supervisory authorities or law enforcement agencies.

(3) Subject persons shall ensure that, upon request, all records maintained in accordance with this regulation are made available to the Financial Intelligence Analysis Unit and, as may be allowed by law, to relevant supervisory authorities and law enforcement agencies, for the purposes of the prevention, detection, analysis and investigation of money laundering and the funding of terrorism.

(4) Subject persons shall have systems in place that enable them to respond fully and efficiently, through secure means that ensure confidentiality, to enquiries from the Financial Intelligence Analysis Unit, relevant supervisory authorities or law enforcement agencies, in accordance with applicable law, as to –

(a) whether they maintain or have maintained during the previous five years a business relationship with a specified natural or legal person; and

(b) the nature of that relationship.

(5) The retention of personal data shall no longer be deemed necessary for the purposes of these regulations beyond the period established in terms of sub-regulation (2) or any extension thereof as may become applicable in terms of the second proviso to sub-regulation (2).

(6) For the purpose of this sub-regulation the term "personal data" shall have the same meaning as is assigned to the term under the Cap. 440. Data Protection Act.

(7) The provisions of this regulation shall be without

prejudice to the right of any other authority in terms of applicable law to access the documents, data and information described in sub-regulation (1)(a) and (b).

Statistical data.

14. (1) The Financial Intelligence Analysis Unit, competent authorities, law enforcement agencies and any other relevant department, agency, authority or body, shall maintain comprehensive statistical data on the national system to combat money laundering or the funding of terrorism to assist in the review of such system and the carrying out of national risk assessments.

(2) Comprehensive statistical data maintained under sub-regulation (1) shall include:

(a) the number of entities and persons conducting a relevant activity or a relevant financial business;

(b) the kind of activity conducted by the entities and persons referred to in (a) above;

(c) economic indicators for each relevant activity and relevant financial business;

(d) the number of suspicious transaction reports made to the Financial Intelligence Analysis Unit and the follow up given to these reports including, where available, data identifying the number and percentage of reports resulting in further investigation;

(e) the number of persons and cases investigated;

(f) the number of persons and cases prosecuted;

(g) the number of persons convicted for the offence of money laundering or the funding of terrorism;

(h) the types of predicate offences, where such information is known;

(i) details and value of property that has been attached, frozen, seized or confiscated;

(j) statistics relevant to the exchange of information between the Financial Intelligence Analysis Unit and foreign counterparts, including data on requests for information made, received, refused and answered in full or in part.

(3) The Financial Intelligence Analysis Unit shall publish consolidated reviews of the statistical data gathered in accordance with this regulation and shall ensure that such statistical data is also made available to the European Commission.

Annex II

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 249

Opinion 2/2017 on data processing at work

Adopted on 8 June 2017

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Contents

1 Executive summary

This Opinion complements the previous Article 29 Working Party ("WP29") publications *Opinion 8/2001 on the processing of personal data in the employment context* (WP48)[1], and the 2002 *Working Document on the surveillance of electronic communications in the workplace* (WP55)[2]. Since the publication of these documents, a number of new technologies have been adopted that enable more systematic processing of employees' personal data at work, creating significant challenges to privacy and data protection.

This Opinion makes a new assessment of the balance between legitimate interests of employers and the reasonable privacy expectations of employees by outlining the risks posed by new technologies and undertaking a proportionality assessment of a number of scenarios in which they could be deployed.

Whilst primarily concerned with the Data Protection Directive, the Opinion looks toward the additional obligations placed on employers by the General Data Protection Regulation. It also restates the position and conclusions of Opinion 8/2001 and the WP55 Working Document, namely that when processing employees' personal data:

- employers should always bear in mind the fundamental data protection principles, irrespective of the technology used;
- the contents of electronic communications made from business premises enjoy the same fundamental rights protections as analogue communications;
- consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence;
- performance of a contract and legitimate interests can sometimes be invoked, provided the processing is strictly necessary for a legitimate purpose and complies with the principles of proportionality and subsidiarity;
- employees should receive effective information about the monitoring that takes place; and
- any international transfer of employee data should take place only where an adequate level of protection is ensured.

2. Introduction

The rapid adoption of new information technologies in the workplace, in terms of infrastructure, applications and smart devices, allows for new types of systematic and potentially invasive data processing at work. For example:

- technologies enabling data processing at work can now be implemented at a fraction of the costs of several years ago whilst the capacity for the processing of personal data by these technologies has increased exponentially;

[1] WP29, *Opinion 08/2001 on the processing of personal data in the employment context*, WP 48, 13 September 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] WP29, *Working document on the surveillance of electronic communications in the workplace*, WP 55, 29 May 2002, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

- new forms of processing, such as those concerning personal data on the use of online services and/or location data from a smart device, are much less visible to employees than other more traditional types such as overt CCTV cameras. This raises questions about the extent to which employees are aware of these technologies, since employers might unlawfully implement these processing without prior notice to the employees; and
- the boundaries between home and work have become increasingly blurred. For example, when employees work remotely (e.g. from home), or whilst they are travelling for business, monitoring of activities outside of the physical working environment can take place and can potentially include monitoring of the individual in a private context.

Therefore, whilst the use of such technologies can be helpful in detecting or preventing the loss of intellectual and material company property, improving the productivity of employees and protecting the personal data for which the data controller is responsible, they also create significant privacy and data protection challenges. As a result, a new assessment is required concerning the balance between the legitimate interest of the employer to protect its business and the reasonable expectation of privacy of the data subjects: the employees.

Whilst this Opinion will focus on new information technologies by assessing nine different scenarios in which they can feature, it will also briefly reflect on more traditional methods of data processing at work where the risks are amplified as a result of technological change.

Where the word "employee" is used in this Opinion, WP29 does not intend to restrict the scope of this term merely to persons with an employment contract recognized as such under applicable labour laws. Over the past decades, new business models served by different types of labour relationships, and in particular employment on a freelance basis, have become more commonplace. This Opinion is intended to cover all situations where there is an employment relationship, regardless of whether this relationship is based on an employment contract.

It is important to state that employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Unless in exceptional situations, employers will have to rely on another legal ground than consent— such as the necessity to process the data for their legitimate interest. However, a legitimate interest in itself is not sufficient to override the rights and freedoms of employees.

Regardless of the legal basis for such processing, a proportionality test should be undertaken prior to its commencement to consider whether the processing is necessary to achieve a legitimate purpose, as well as the measures that have to be taken to ensure that infringements of the rights to private life and secrecy of communications are limited to a minimum. This can form part of a Data Protection Impact Assessment (DPIA).

3. The legal framework

Whilst the analysis below is primarily conducted in relation to the current legal framework under Directive 95/46/EC (the Data Protection Directive or "DPD")[3] , this Opinion will also

[3] 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 on the free movement of such data, *OJ L 281, 23/11/1995, p.31-50*, url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

look toward the obligations under Regulation 2016/679 (the General Data Protection Regulation or "GDPR")[4], which has already entered into force and which will become applicable on 25 May 2018.

With regard to the proposed ePrivacy Regulation[5], the Working Party calls on European legislators to create a specific exception for interference with devices issued to employees[6]. The Proposed Regulation does not contain a suitable exception to the general interference prohibition, and employers cannot usually provide valid consent for the processing of personal data of their employees.

3.1 Directive 95/46/EC—Data Protection Directive ("DPD")

In Opinion 08/2001, WP29 previously outlined that employers take into account the fundamental data protection principles of the DPD when processing personal data in the employment context. The development of new technologies and new methods of processing in this context have not altered this situation—in fact, it can be said that such developments have made it *more* important for employers to do so. In this context, employers should:

- ensure that data is processed for specified and legitimate purposes that are proportionate and necessary;
- take into account the principle of purpose limitation, while making sure that the data are adequate, relevant and not excessive for the legitimate purpose;
- apply the principles of proportionality and subsidiarity regardless of the applicable legal ground;
- be transparent with employees about the use and purposes of monitoring technologies;
- enable the exercise of data subject rights, including the rights of access and, as appropriate, the rectification, erasure or blocking of personal data;
- keep the data accurate, and not retain them any longer than necessary; and
- take all necessary measures to protect the data against unauthorised access and ensure that staff are sufficiently aware of data protection obligations.

Without repeating the earlier advice given, WP29 wishes to highlight three principles, namely: legal grounds, transparency, and automated decisions.

3.1.1 *Legal grounds (Article 7)*

When processing personal data in the employment context, at least one of the criteria set out in Art. 7 has to be satisfied. If the types of personal data processed involve the special categories(as elaborated in Art. 8), the processing is prohibited unless an exception applies[7,8].

[4] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1-88*, url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[5] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] See WP29, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation*, WP 247, 04 April 2017, page 29; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

[7] As stated in part 8 of Opinion 08/2001; for example, Art. 8(2)(b) provides an exception for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards.

Even if the employer can rely on one of those exceptions, a legal ground from Art. 7 is still required for the processing to be legitimate.

In summary, employers must therefore take note of the following:

- for the majority of such data processing at work**, the legal basis cannot and should not be the consent of the employees** (Art 7(a)) due to the nature of the relationship between employer and employee;
- processing may be necessary for **the performance of a contract** (Art 7(b)) in cases where the employer has to process personal data of the employee to meet any such obligations;
- it is quite common that **employment law may impose legal obligations** (Art. 7(c)) **that necessitate the processing of personal data**; in such cases the employee must be clearly and fully informed of such processing (unless an exception applies);
- should an employer seek to rely on **legitimate interest** (Art. 7(f)) the purpose of the processing must be legitimate; the chosen method or specific technology must be necessary, proportionate and implemented in the least intrusive manner possible along with the ability to enable the employer to demonstrate that **appropriate measures have been put in place** to ensure a balance with the fundamental rights and freedoms of employees[9];
- the processing operations must also comply with the **transparency requirements** (Art. 10 and 11), and employees should be clearly and fully informed of the processing of their personal data[10], including the existence of any monitoring; and
- **appropriate technical and organisational measures** should be adopted to ensure security of the processing (Art. 17).

The most relevant criteria under Art. 7 are detailed below.

- **Consent (Article 7(a))**

Consent, according to the DPD, is defined as any freely-given, specific and informed indication of a data subject's wishes by which the he or she signifies his or her agreement to personal data relating to them being processed. For consent to be valid, it must also be revocable.

WP29 has previously outlined in Opinion 8/2001 that where an employer has to process personal data of his/her employees it is misleading to start with the supposition that the processing can be legitimised through the employees' consent. In cases where an employer says they require consent and there is a real or potential relevant prejudice that arises from the employee not consenting (which can be highly probable in the employment context, especially when it concerns the employer tracking the behaviour of the employee over time), then the consent is not valid since it is not and cannot be freely given. Thus, for the

[8] It should be noted that in some countries, there are special measures in place that employers must abide by to protect employees' private lives. Portugal is one example of countries where such special measures exist and similar measures may apply in some other Member States too. The conclusions in section 5.6 as well as the examples presented in sections 5.1 and 5.7.1 of this Opinion are therefore not valid in Portugal for these reasons.

[9] WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, adopted 9 April 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[8] [10] Pursuant to Art. 11(2) of the DPD, the controller is exempted from the obligation to provide information to the data subject in cases where the recording or collection of data is expressly laid down by law.

majority of the cases of employees' data processing, the legal basis of that processing cannot and should not be the consent of the employees, so a different legal basis is required.

Moreover, even in cases where consent could be said to constitute a valid legal basis of such a processing (i.e. if it can be undoubtedly concluded that the consent is freely given), it needs to be a specific and informed indication of the employee's wishes. Default settings on devices and/or the installation of software that facilitate the electronic personal data processing cannot qualify as consent given from employees, since consent requires an active expression of will. A lack of action (i.e, not changing the default settings) may generally not be considered as a specific consent to allow such processing[11].

- **Performance of a contract (Article 7(b))**

Employment relationships are often based on a contract of employment between the employer and the employee. When meeting obligations under this contract, such as paying the employee, the employer is required to process some personal data.

- **Legal obligations (Article 7(c))**

It is quite common that employment law imposes legal obligations on the employer, which necessitate the processing of personal data (e.g. for the purpose of tax calculation and salary administration). Clearly, in such cases, such a law constitutes the legal basis for the data processing..

- **Legitimate interest (Article 7(f))**

If an employer wishes to rely upon the legal ground of Art. 7(f) of the DPD, the purpose of the processing must be legitimate, and the chosen method or specific technology with which the processing is to be undertaken must be necessary for the legitimate interest of the employer. The processing must also be proportionate to the business needs, i.e. the purpose, it is meant to address. Data processing at work should be carried out in the least intrusive manner possible and be targeted to the specific area of risk. Additionally, if relying on Art. 7(f), the employee retains the right to object to the processing on compelling legitimate grounds under Art. 14.

In order to rely on Art. 7(f) as the legal ground for processing it is essential that specific mitigating measures are present to ensure a proper balance between the legitimate interest of the employer and the fundamental rights and freedoms of the employees.[12] Such measures, depending on the form of monitoring, should include limitations on monitoring so as to guarantee that the employee's privacy is not violated. Such limitations could be:

[11] See also WP29, *Opinion 15/2011 on the definition of consent,* WP187, 13 July 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, page 24.

[12] For an example of the balance that needs to be struck, see the case of *Köpke v Germany*, [2010] ECHR 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), in which an employee was dismissed as a result of a covert video surveillance operation undertaken by the employer and a private detective agency. Whilst in this instance the Court concluded that the domestic authorities had struck a fair balance between the employer's legitimate interest (in the protection of its property rights), the employee's right to respect for private life, and the public interest in the administration of justice, it also observed that the various interests concerned could be given a different weight in future as a result of technological development

- geographical (e.g. monitoring only in specific places; monitoring sensitive areas such as religious places and for example sanitary zones and break rooms should be prohibited),
- data-oriented (e.g. personal electronic files and communication should not be monitored), and
- time-related (e.g. sampling instead of continuous monitoring).

3.1.2 *TRANSPARENCY (ARTICLES 10 AND 11)*

The transparency requirements of Articles 10 and 11 apply to data processing at work; employees must be informed of the existence of any monitoring, the purposes for which personal data are to be processed and any other information necessary to guarantee fair processing.

With new technologies, the need for transparency becomes more evident since they enable the collection and further processing of possibly huge amounts of personal data in a covert way.

3.1.3 *AUTOMATED DECISIONS (ARTICLE 15)*

Art. 15 of the DPD also grants data subjects the right not to be subject to a decision based solely on automated processing, where that decision produces legal effects or similarly significantly affects them and which is based solely on automated processing of data intended to evaluate certain personal aspects, such as performance at work, unless the decision is necessary for entering into or performance of a contract, authorised by Union or Member State law, or is based on the explicit consent of the data subject.

3.2 Regulation 2016/679—General Data Protection Regulation ("GDPR")

The GDPR includes and enhances the requirements in the DPD. It also introduces new obligations for all data controllers, including employers.

3.2.1 *DATA PROTECTION BY DESIGN*

Art. 25 of the GDPR requires data controllers to implement data protection by design and by default. As an example: where an employer issues devices to employees, the most privacy-friendly solutions should be selected if tracking technologies are involved. Data minimisation must also be taken into account.

3.2.2 *DATA PROTECTION IMPACT ASSESSMENTS*

Art. 35 of the GDPR outlines the requirements for a data controller to carry out a Data Protection Impact Assessment (DPIA) where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing itself, is likely to result in a high risk to the rights and freedoms of natural persons. An example is a case of systematic and extensive evaluation of personal aspects related to natural persons based on automated processing including profiling, and on which decisions are taken that produce legal effects concerning the natural person or similarly significantly affect the natural person.

Where the DPIA indicates that the identified risks cannot be sufficiently addressed by the controller—i.e., that the residual risks remain high—then the controller must consult the supervisory authority prior to the commencement of the processing (Art. 36(1)) as clarified in the WP29 guidelines on DPIAs[13].

3.2.2 "*PROCESSING IN THE CONTEXT OF EMPLOYMENT*"

Art. 88 of the GDPR states that Member States may, by law or collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context. In particular, these rules may be provided for the purposes of:

- recruitment;
- performance of the employment contract (including discharge of obligations laid down by law or collective agreements);
- management, planning and organisation of work;
- equality and diversity in the workplace;
- health and safety at work;
- protection of an employer's or customer's property;
- exercise and enjoyment (on an individual basis) of rights and benefits related to employment; and
- termination of the employment relationship.

In accordance with Art. 88(2), any such rules should include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to:

- the transparency of processing;
- the transfer of personal data within a group of undertakings or group of enterprises engaged in a joint economic activity; and
- monitoring systems at the workplace.

In this Opinion, the Working Party has provided guidelines for the legitimate use of new technology in a number of specific situations, detailing suitable and specific measures to safeguard the human dignity, legitimate interest and fundamental rights of employees.

4. Risks

Modern technologies enable employees to be tracked over time, across workplaces and their homes, through many different devices such as smartphones, desktops, tablets, vehicles and wearables. If there are no limits to the processing, and if it is not transparent, there is a high risk that the legitimate interest of employers in the improvement of efficiency and the protection of company assets turns into unjustifiable and intrusive monitoring.

Technologies that monitor communications can also have a chilling effect on the fundamental rights of employees to organise, set up workers' meetings, and to communicate confidentially (including the right to seek information). Monitoring

[13] WP29, *Guidelines on data protection impact assessment (DPIA) and determining whether processing is likely to result in "high risk" for the purposes of Regulation 2016/679*, WP 248, 04 April 2017, url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, page 18.

communications and behaviour will put pressure on employees to conform in order to prevent the detection of what might be perceived as anomalies, in a comparable way to the way in which the intensive use of CCTV has influenced citizens' behaviour in public spaces. Moreover, owing to the capabilities of such technologies, employees may not be aware of what personal data are being processed and for which purposes, whilst it is also possible that they are not even aware of the existence of the monitoring technology itself.

Monitoring IT usage also differs from other, more visible observation and monitoring tools like CCTV in that it can take place in a covert way. In the absence of an easily understandable and readily accessible workplace monitoring policy, employees may not be aware of the existence and consequences of the monitoring that is taking place, and are therefore unable to exercise their rights. A further risk comes from the "over-collection" of data in such systems, e.g. those collecting WiFi location data.

The increase in the amount of data generated in the workplace environment, in combination with new techniques for data analysis and cross-matching, may also create risks of incompatible further processing. Examples of illegitimate further processing include using systems that are legitimately installed to protect properties to then monitor the availability, performance and customer-friendliness of employees. Others include using data collected via a CCTV system to regularly monitor the behaviour and performance of employees, or using data of a geolocation system (such as for example WiFi- or Bluetooth tracking) to constantly check an employee's movements and behaviour.

As a result, such tracking may infringe upon the privacy rights of employees, regardless of whether the monitoring takes place systematically or occasionally. The risk is not limited to the analysis of the content of communications. Thus, the analysis of metadata about a person might allow for an equally privacy-invasive detailed monitoring of an individual's life and behavioural patterns.

The extensive use of monitoring technologies may also limit employees' willingness to (and channels by which they could) inform employers about irregularities or illegal actions of superiors and/or other employees threatening to damage the business (especially client data) or workplace. Anonymity is often necessary for a concerned employee to take action and report such situations. Monitoring that infringes upon the privacy rights of employees may hamper necessary communications to the appropriate officers. In such an instance, the established means for internal whistle-blowers may become ineffective[14][14].

5. Scenarios

This section addresses a number of data processing at work scenarios in which new technologies and/or developments of existing technologies have, or may have, the potential to result in high risks to the privacy of employees. In all such cases employers should consider whether:

[14] See for example WP29, *Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*, WP 117, 1 February 2006, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

- the processing activity is necessary, and if so, the legal grounds that apply;
- the proposed processing of personal data is fair to the employees;
- the processing activity is proportionate to the concerns raised; and
- the processing activity is transparent.

5.1 Processing operations during the recruitment process

Use of social media by individuals is widespread and it is relatively common for user profiles to be publicly viewable depending on the settings chosen by the account holder. As a result, employers may believe that inspecting the social profiles of prospective candidates can be justified during their recruitment processes. This may also be the case for other publicly-available information about the potential employee.

However, employers should not assume that merely because an individual's social media profile is publicly available they are then allowed to process those data for their own purposes. A legal ground is required for this processing, such as legitimate interest. In this context the employer should—prior to the inspection of a social media profile—take into account whether the social media profile of the applicant is related to business or private purposes, as this can be an important indication for the legal admissibility of the data inspection. In addition, employers are only allowed to collect and process personal data relating to job applicants to the extent that the collection of those data is necessary and relevant to the performance of the job which is being applied for.

Data collected during the recruitment process should generally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the individual concerned[15]. The individual must also be correctly informed of any such processing before they engage with the recruitment process.

There is no legal ground for an employer to require potential employees to "friend" the potential employer, or in other ways provide access to the contents of their profiles.

Example

During the recruitment of new staff, an employer checks the profiles of the candidates on various social networks and includes information from these networks (and any other information available on the internet) in the screening process.

Only if it is necessary for the job to review information about a candidate on social media, for example in order to be able to assess specific risks regarding candidates for a specific function, and the candidates are correctly informed (for example, in the text of the job advert) the employer may have a legal basis under Article 7(f) to review publicly-available information about candidates.

[15] See also Council of Europe, *Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment*, paragraph 13.2 (1 April 2015, url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). In cases where the employer wishes to retain the data with a view to a further job opportunity, the data subject should be informed accordingly and be given the possibility to object to such further processing, in which case it should be deleted (Id.).

5.2 Processing operations resulting from in-employment screening

Through the existence of profiles on social media, and the development of new analytical technologies, employers have (or can obtain) the technical capability of permanently screening employees by collecting information regarding their friends, opinions, beliefs, interests, habits, whereabouts, attitudes and behaviours therefore capturing data, including sensitive data, relating to the employee's private and family life.

In-employment screening of employees' social media profiles should not take place on a generalised basis.

Moreover, employers should refrain from requiring an employee or a job applicant access to information that he or she shares with others through social networking.

Example
An employer monitors the LinkedIn profiles of former employees that are involved during the duration of non-compete clauses. The purpose of this monitoring is to monitor compliance with such clauses. The monitoring is limited to these former employees.

As long as the employer can prove that such monitoring is necessary to protect his legitimate interests, that there are no other, less invasive means available, and that the former employees have been adequately informed about the extent of the regular observation of their public communications, the employer may be able to rely on the legal basis of Article 7(f) of the DPD.

Additionally, employees should not be required to utilise a social media profile that is provided by their employer. Even when this is specifically foreseen in light of their tasks (e.g. spokesperson for an organisation), they must retain the option of a "non-work" non-public profile that they can use instead of the "official" employer-related profile, and this should be specified in the terms and conditions of the employment contract.

5.3 Processing operations resulting from monitoring ICT usage at the workplace

Traditionally, the monitoring of electronic communications in the workplace (eg, phone, internet browsing, email, instant messaging, VOIP, etc.) was considered the main threat to employees' privacy. In its 2001 *Working Document on the surveillance of electronic communications in the workplace*, WP29 made a number of conclusions in relation to the monitoring of email and internet usage. While those conclusions remain valid, there is a need to take into account technological developments that have enabled newer, potentially more intrusive and pervasive ways of monitoring. Such developments include, amongst others:

- Data Loss Prevention (DLP) tools, which monitor outgoing communications for the purpose of detecting potential data breaches;
- Next-Generation Firewalls (NGFWs) and Unified Threat Management (UTM) systems, which can provide a variety of monitoring technologies including deep packet inspection, TLS interception, website filtering, content filtering, on-appliance reporting, user identity information and (as described above) data loss prevention. Such technologies may also be deployed individually, depending on the employer;

- security applications and measures that involve logging employee access to the employer's systems;
- eDiscovery technology, which refers to any process in which electronic data is searched with the aim of its use as evidence;
- tracking of application and device usage via unseen software, either on the desktop or in the cloud;
- the use in the workplace of office applications provided as a cloud service, which in theory allow for very detailed logging of the activities of employees;
- monitoring of personal devices (e.g., PCs, mobile phones, tablets), that employees supply for their work in accordance with a specific use policy, such as Bring-Your-Own-Device (BYOD), as well as Mobile Device Management (MDM) technology which enables the distribution of applications, data and configuration settings, and patches for mobile devices; and
- the use of wearable devices (e.g., health and fitness devices).

It is possible that an employer will implement an "all-in-one" monitoring solution, such as a suite of security packages which enable them to monitor all ICT usage in the workplace as opposed to just email and/or website monitoring as was once the case. The conclusions adopted in WP55 would apply for any system that enables such monitoring to take place.[16]

Example

An employer intends to deploy a TLS inspection appliance to decrypt and inspect secure traffic, with the purpose of detecting anything malicious. The appliance is also able to record and analyse the entirety of an employee's online activity on the organisation's network.

Use of encrypted communications protocols is increasingly being implemented to protect online data flows involving personal data against interception. However, this can also present issues, as the encryption makes it impossible to monitor incoming and outgoing data. TLS inspection equipment decrypts the data stream, analyses the content for security purposes and then re-encrypts the stream afterwards.

In this example, the employer relies upon legitimate interests—the necessity to protect the network, and the personal data of employees and customers held within that network, against unauthorised access or data leakage. However, monitoring every online activity of the employees is a disproportionate response and an interference with the right to secrecy of communications. The employer should first investigate other, less invasive, means to protect the confidentiality of customer data and the security of the network.

To the extent that some interception of TLS traffic can be qualified as strictly necessary, the appliance should be configured in a way to prevent permanent logging of employee activity, for example by blocking suspicious incoming or outgoing traffic and redirecting the user to an information portal where he or she may ask for review of such an automated decision. If some general logging would nonetheless be deemed strictly necessary, the appliance may

[16] See also *Copland v United Kingdom,* (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), in which the Court stated that emails sent from business premises and information derived from the monitoring of internet use could be a part of an employee's private life and correspondence, and that the collection and storage of that information without the knowledge of the employee would amount to an interference with the employee's rights, although the Court did not rule that such monitoring would never be necessary in a democratic society.

also be configured not to store log data unless the appliance signals the occurrence of an incident, with a minimization of the information collected.

As a good practice, the employer could offer alternative unmonitored access for employees. This could be done by offering free WiFi, or stand-alone devices or terminals (with appropriate safeguards to ensure confidentiality of the communications) where employees can exercise their legitimate right to use work facilities for some private usage[17]. Moreover, employers should consider certain types of traffic whose interception endangers the proper balance between their legitimate interests and employee's privacy—such as the use of private webmail, visits to online banking and health websites—with the aim to appropriately configure the appliance so as not to proceed with interception of communications in circumstances that are not compliant with proportionality. Information on the type of communications that the appliance is monitoring should be specified to the employees.

A policy concerning the purposes for when, and by whom, suspicious log data can be accessed should be developed and made easily and permanently accessible for all employees, in order to also guide them about acceptable and unacceptable use of the network and facilities. This allows employees to adapt their behaviour to prevent being monitored when they legitimately use IT work facilities for private use. As good practice, such a policy should be evaluated, at least annually, to assess whether the chosen monitoring solution delivers the intended results, and whether there are other, less invasive tools or means available to achieve the same purposes.

Irrespective of the technology concerned or the capabilities it possesses, the legal basis of Article 7(f) is only available if the processing meets certain conditions. Firstly, employers utilising these products and applications must consider the proportionality of the measures they are implementing, and whether any additional actions can be taken to mitigate or reduce the scale and impact of the data processing. As an example of good practice, this consideration could be undertaken via a DPIA prior to the introduction of any monitoring technology. Secondly, employers must implement and communicate acceptable use policies alongside privacy policies, outlining the permissible use of the organisation's network and equipment, and strictly detailing the processing taking place.

In some countries the creation of such a policy would legally require approval of a Workers' Council or similar representation of employees. In practice, such policies are often drafted by IT maintenance staff. Since their main focus will mostly be on security, and not on the legitimate expectation of privacy of employees, WP29 recommends that in all cases a representative sample of employees is involved in assessing the necessity of the monitoring, as well as the logic and accessibility of the policy.

[17] See Halford v. United Kingdom, [1997] ECHR 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), in which the Court stated that "telephone calls made from business premises as well as from the home may be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8 paragraph 1 [of the Convention]"; and Barbulescu v. Romania, [2016] ECHR 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), concerning the use of a professional instant messenger account for personal correspondence, in which the Court stated that monitoring of the account by the employer was limited and proportionate; the dissenting opinion of Judge Pinto de Alberquerque which argued for a careful balance to be struck

Example

An employer deploys a Data Loss Prevention tool to monitor the outgoing e-mails automatically, for the purpose of preventing unauthorised transmission of proprietary data (e.g. customer's personal data), independently from whether such an action is unintentional or not. Once an e-mail is being considered as the potential source of a data breach, further investigation is performed.

Again, the employer relies upon the necessity for his legitimate interest to protect the personal data of customers as well as his assets against unauthorised access or data leakage. However, such a DLP tool may involve unnecessary processing of personal data — for example, a "false positive" alert might result in unauthorized access of legitimate e-mails that have been sent by employees (which may be, for instance, personal e-mails).

Therefore, the necessity of the DLP tool and its deployment should be fully justified so as to strike the proper balance between his legitimate interests and the fundamental right to the protection of employees' personal data. In order for the legitimate interests of the employer to be relied upon, certain measures should be taken to mitigate the risks. For example, the rules that the system follows to characterize an e-mail as potential data breach should be fully transparent to the users, and in cases that the tool recognises an e-mail that is to be sent as a possible data breach, a warning message should inform the sender of the e-mail prior to the e-mail transmission, so as to give the sender the option to cancel this transmission.

In some cases, the monitoring of employees is possible not so much because of the deployment of specific technologies, but simply because employees are expected to use online applications made available by the employer which process personal data. The use of cloud-based office applications (e.g. document editors, calendars, social networking) is an example of this. It should be ensured that employees can designate certain private spaces to which the employer may not gain access unless under exceptional circumstances. This, for example, is relevant for calendars, which are often also used for private appointments. If the employee sets an appointment to "Private" or notes this in appointment itself, employers (and other employees) should not be allowed to review the contents of the appointment.

The requirement of subsidiarity in this context sometimes means that no monitoring may take place at all. For example, this is the case where the prohibited use of communications services can be prevented by blocking certain websites. If it is possible to block websites, instead of continuously monitoring all communications, blocking should be chosen in order to comply with this requirement of subsidiarity.

More generally, prevention should be given much more weight than detection—the interests of the employer are better served by preventing internet misuse through technical means than by expending resources in detecting misuse.

5.4 Processing operations resulting from monitoring ICT usage outside the workplace

ICT usage outside the workplace has become more common with the growth of homeworking, remote working and "bring your own device" policies. The capabilities of such technologies can pose a risk to the private life of employees, as in many cases the monitoring systems existing in the workplace are effectively extended into the employees' domestic sphere when they use such equipment. .

5.4.1 *MONITORING OF HOME AND REMOTE WORKING*

It has become more common for employers to offer employees the option to work remotely, e.g., from home and/or whilst in transit. Indeed, this is a central factor behind the reduced distinction between the workplace and the home. In general this involves the employer issuing ICT equipment or software to the employees which, once installed in their home/on their own devices, enables them to have the same level of access to the employer's network, systems and resources that they would have if they were in the workplace, depending on the implementation.

Whilst remote working can be a positive development, it also presents an area of additional risk for an employer. For example, employees that have remote access to the employer's infrastructure are not bound by the physical security measures that may be in place at the employer's premises. To put it plainly: without the implementation of appropriate technical measures the risk of unauthorised access increases and may result in the loss or destruction of information, including personal data of employees or customers, which the employer may hold.

In order to mitigate this area of risk employers may think there is a justification for deploying software packages (either on-premise or in the cloud) that have the capabilities of, for example, logging keystrokes and mouse movements, screen capturing (either randomly or at set intervals), logging of applications used (and how long they were used for), and, upon compatible devices, enabling webcams and collecting the footage thereof. Such technologies are widely available including from third parties such as cloud providers.

However, the processing involved in such technologies are disproportionate and the employer is very unlikely to have a legal ground under legitimate interest, e.g. for recording an employee's keystrokes and mouse movements.

The key is addressing the risk posed by home and remote working in a proportionate, non-excessive manner, in whatever way the option is offered and by whatever technology is proposed, particularly if the boundaries between business and private use are fluid.

5.4.2 *BRING YOUR OWN DEVICE (BYOD)*

Due to the rise in popularity, features and capability of consumer electronic devices, employers may face demands from employees to use their own devices in the workplace to carry out their jobs. This is known as "bring your own device" or BYOD.

Implementing BYOD effectively can lead to a number of benefits for employees, including improved employee job satisfaction, overall morale increase, increased job efficiency and increased flexibility. However, by definition, some use of an employee's device will be personal in nature, and this is more likely to be the case at certain times of the day (e.g., evenings and weekends). It is therefore a distinct possibility that employees' use of their own devices will lead to employers processing non-corporate information about those employees, and possibly any family members who also use the devices in question.

In the employment context, BYOD privacy risks are commonly associated with monitoring technologies that collect identifiers such as MAC addresses, or in instances where an employer accesses an employee's device under the justification of performing a security scan, i.e. for malware. In respect of the latter, a number of commercial solutions exist that allow for the scanning of private devices, however their usage could potentially

access all data on that device and therefore they must be carefully managed. For example, those sections of a device which are presumed to be only used for private purposes (e.g. the folder storing photos taken with the device) may in principle not be accessed.

Monitoring the location and traffic of such devices may be considered to serve a legitimate interest to protect the personal data that the employer is responsible for as the data controller; however this may be unlawful where an employee's personal device is concerned, if such monitoring also captures data relating to the employee's private and family life. In order to prevent monitoring of private information appropriate measures must be in place to distinguish between private and business use of the device.

Employers should also implement methods by which their own data on the device is securely transferred between that device and their network. It may be the case that the device is therefore configured to route all traffic through a VPN back into the corporate network, so as to offer a certain level of security; however, if such a measure is used, the employer should also consider that software installed for the purposes of monitoring pose a privacy risk during periods of personal usage by the employee. Devices that offer additional protections such as "sandboxing" data (keeping data contained within a specific app) could be used.

Conversely, the employer must also consider the prohibition of the use of specific work devices for private use if there is no way to prevent private use being monitored—for example if the device offers remote access to personal data for which the employer is the data controller.

5.4.3 *MOBILE DEVICE MANAGEMENT (MDM)*

Mobile device management enables employers to locate devices remotely, deploy specific configurations and/or applications, and delete data on demand. An employer may operate this functionality himself, or use a third party to do so. MDM services also enable employers to record or track the device in real-time even if it is not reported stolen.

A DPIA should be performed prior to the deployment of any such technology where it is new, or new to the data controller. If the outcome of the DPIA is that the MDM technology is necessary in specific circumstances, an assessment should still be made as to whether the resulting data processing complies with the principles of proportionality and subsidiarity. Employers must ensure that the data collected as part of this remote location capability is processed for a specified purpose and does not, and could not, form part of a wider programme enabling ongoing monitoring of employees. Even for specified purposes, the tracking features should be mitigated. Tracking systems can be designed to register the location data without presenting it to the employer—in such circumstances, the location data should become available only in circumstances where the device would be reported or lost.

Employees whose devices are enrolled in MDM services must also be fully informed as to what tracking is taking place, and what consequences this has for them.

5.4.4 *WEARABLE DEVICES*

Employers are increasingly tempted to provide wearable devices to their employees in order to track and monitor their health and activity within and sometimes even outside of the

workplace. However, this data processing involves the processing of health data, and is therefore prohibited based on Article 8 of the DPD.

Given the unequal relationship between employers and employees—i.e., the employee has a financial dependence on the employer—and the sensitive nature of the health data, it is highly unlikely that legally valid explicit consent can be given for the tracking or monitoring of such data as employees are essentially not 'free' to give such consent in the first place. Even if the employer uses a third party to collect the health data, which would only provide aggregated information about general health developments to the employer, the processing would still be unlawful.

Also, as described in *Opinion 5/2014 on Anonymisation Techniques*[18], it is technically very difficult to ensure complete anonymisation of the data. Even in an environment with over a thousand employees, given the availability of other data about the employees the employer would still be able to single out individual employees with particular health indications such as high blood pressure or obesity.

Example:

An organisation offers fitness monitoring devices to its employees as a general gift. The devices count the number of steps employees take, and register their heartbeats and sleeping patterns over time.

The resulting health data should only be accessible to the employee and not the employer. Any data transferred between the employee (as data subject) and the device/service provider (as data controller) is a matter for those parties.

As the health data could also be processed by the commercial party that has manufactured the devices or offers a service to employers, when choosing the device or service the employer should evaluate the privacy policy of the manufacturer and/or service provider, to ensure that it does not result in unlawful processing of health data on employees.

5.5 Processing operations relating to time and attendance

Systems that enable employers to control who can enter their premises, and/or certain areas within their premises, can also allow the tracking of employees' activities. Although such systems have existed for a number of years, new technologies intended to track employees' time and attendance are being more widely deployed, including those that process of biometric data as well as others such as mobile device tracking.

Whilst such systems can form an important component of an employer's audit trail, they also pose the risk of providing an invasive level of knowledge and control regarding the activities of the employee whilst in the workplace.

[18] WP29, Opinion 5/2014 on anonymization techniques, WP 216, 10 April 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Example:

An employer maintains a server room in which business-sensitive data, personal data relating to employees and personal data relating to customers is stored in digital form. In order to comply with legal obligations to secure the data against unauthorised access, the employer has installed an access control system that records the entrance and exit of employees who have appropriate permission to enter the room. Should any item of equipment go missing, or if any data is subject to unauthorised access, loss or theft, the records maintained by the employer allow them to determine who had access to the room at that time.

Given that the processing is necessary and does not outweigh the right to private life of the employees, it can be in the legitimate interest under Art. 7(f), if the employees have been adequately informed about the processing operation. However, the continuous monitoring of the frequency and exact entrance and exit times of the employees cannot be justified if these data are also used for another purpose, such as employee performance evaluation.

5.6 Processing operations using video monitoring systems

Video monitoring and surveillance continues to present similar issues for employee privacy as before: the capability to continuously capture the behaviour of the worker.[19] The most relevant changes relating to the application of this technology in the employment context are the capability to access the collected data remotely (e.g. via a smartphone) easily; the reduction in the cameras' sizes (along with an increase in their capabilities, e.g. high-definition); and the processing that can be performed by new video analytics.

With the capabilities given by video analytics, it is possible for an employer to monitor the worker's facial expressions by automated means, to identify deviations from predefined movement patterns (e.g. factory context), and more. This would be disproportionate to the rights and freedoms of employees, and therefore, generally unlawful. The processing is also likely to involve profiling, and possibly, automated decision-making. Therefore, employers should refrain from the use of facial recognition technologies. There may be some fringe exceptions to this rule, but such scenarios cannot be used to invoke a general legitimation of the use of such technology[20].

5.7 Processing operations involving vehicles used by employees

Technologies that enable employers to monitor their vehicles have become widely adopted, particularly among organisations whose activities involve transport or have significant vehicle fleets.

Any employer using vehicle telematics will be collecting data about both the vehicle and the individual employee using that vehicle. This data can include not just the location of the vehicle (and, hence, the employee) collected by basic GPS tracking systems, but, depending on the technology, a wealth of other information including driving behaviour. Certain

[19] See the above referenced case of *Köpke v Germany*; additionally, it should also be noted that in some jurisdictions the installation of systems such as CCTV for the purpose of proving unlawful conduct has been ruled permissible; see the case of *Bershka* in the Constitutional Court of Spain.

[20] Moreover, under the GDPR, processing of biometric data for identification purposes must be based on an exception provided by Art. 9(2).

technologies can also enable continuous monitoring both of the vehicle and the driver (eg, event data recorders).

An employer might be obliged to install tracking technology in vehicles to demonstrate compliance with other legal obligations, e.g. to ensure the safety of employees who drive those vehicles. The employer may also have a legitimate interest in being able to locate the vehicles at any time. Even if employers would have a legitimate interest to achieve these purposes, it should first be assessed whether the processing for these purposes is necessary, and whether the actual implementation complies with the principles of proportionality and subsidiarity. Where private use of a professional vehicle is allowed, the most important measure an employer can take to ensure compliance with these principles is the offering of an opt-out: the employee in principle should have the option to temporarily turn off location tracking when special circumstances justify this turning off, such as a visit to a doctor. This way, the employee can on its own initiative protect certain location data as private. The employer must ensure that the collected data are not used for illegitimate further processing, such as the tracking and evaluation of employees.

The employer must also clearly inform the employees that a tracking device has been installed in a company vehicle that they are driving, and that their movements are being recorded whilst they are using that vehicle (and that, depending on the technology involved, their driving behaviour may also be recorded). Preferably such information should be displayed prominently in every car, within eyesight of the driver.

It is possible that employees may use company vehicles outside working hours, e.g. for personal use, depending on the specific policies governing the use of those vehicles. Given the sensitivity of location data, it is unlikely that there is a legal basis for monitoring the locations of employees' vehicles outside agreed working hours. However, should such a necessity exist, an implementation that would be proportionate to the risks should be considered. For example, this could mean that, in order to prevent car theft, the location of the car is not registered outside working hours, unless the vehicle leaves a widely defined circle (region or even country). In addition, the location would only be shown in a "break-the-glass" way—the employer would only activate the "visibility" of the location, accessing the data already stored by the system, when the vehicle leaves a predefined region.

As stated in the WP29 *Opinion 13/2011 on Geolocation services on smart mobile devices*[21]:

"Vehicle tracking devices are not staff tracking devices. Their function is to track or monitor the location of the vehicles in which they are installed. Employers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example by sending alerts in relation to speed of vehicle."

Further, as stated in the WP29 *Opinion 5/2005 on the use of location data with a view to providing value-added services*[22]:

[21] WP29, *Opinion 13/2011 on Geolocation services on smart mobile devices,* WP 185, 16 May 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[22] WP29, *Opinion 5/2005 on the use of location data with a view to providing value-added services*, WP 115, 25 November 2005, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

"Processing location data can be justified where it is done as part of monitoring the transport of people or goods or improving the distribution of resources for services in scattered locations (e.g. planning operations in real time), or where a security objective is being pursued in relation to the employee himself or to the goods or vehicles in his charge. Conversely, the Working Party considers data processing to be excessive where employees are free to organise their travel arrangements as they wish or where it is done for the sole purpose of monitoring an employee's work where this can be monitored by other means."

5.7.1 EVENT DATA RECORDERS

Event data recorders provide an employer with the technical capability of processing a significant amount of personal data about the employees that drive company vehicles. Such devices are increasingly being placed into vehicles with the goal to record video, possibly including sound, in case of an accident. These systems are able to record at certain times, e.g. in response to sudden braking, abrupt directional change or accidents, where the moments immediately preceding the incident are stored, but they can also be set to monitor continuously. This information can be used subsequently to observe and review an individual's driving behaviour with the aim of improving it. Moreover, many of these systems include GPS to track the location of the vehicle in real-time and other details corresponding to the driving (such as the vehicle speed) can be also stored for further processing.

These devices have become particularly prevalent among organisations whose activities involve transport or have significant vehicle fleets. However, the deployment of event data recorders can only be lawful if there is a necessity to process the ensuing personal data about the employee for a legitimate purpose, and the processing complies with the principles of proportionality and subsidiarity.

Example
A transport company equips all of its vehicles with a video camera inside the cabin which records sound and video. The purpose of processing these data is to improve the driving skills of the employees. The cameras are configured to retain recordings whenever incidents such as sudden braking or abrupt directional change take place. The company assumes it has a legal ground for the processing in its legitimate interest under Article 7(f) of the Directive, to protect the safety of its employees and other drivers' safety.

However, the legitimate interest of the company to monitor the drivers does not prevail over the rights of those drivers to the protection of their personal data. The continuous monitoring of employees with such cameras constitutes a serious interference with their right of privacy. There are other methods (e.g., the installation of equipment that prevents the use of mobile phones) as well as other safety systems like an advanced emergency braking system or a lane departure warning system that can be used for the prevention of vehicle accidents which may be more appropriate. Furthermore, such a video has a high probability of resulting in the processing of personal data of third parties (such as pedestrians) and, for such a processing, the legitimate interest of the company is not sufficient to justify the processing.

5.8 Processing operations involving disclosure of employee data to third parties

It has become increasingly common for companies to transmit their employees' data to their customers for the purpose of ensuring reliable service provision. These data may be quite excessive depending on the scope of services provided (e.g. an employee's photo may be included). However, employees are not in a position, given the imbalance of power, to give free consent to the processing of their personal data by their employer, and if the data processing is not proportional, the employer does not have a legal ground.

Example:

A delivery company sends its customers an e-mail with a link to the name and the location of the deliverer (employee). The company also intended to provide a passport photo of the deliverer. The company assumed it would have a legal ground for the processing in its legitimate interest (Article 7(f) of the Directive), allowing the customer to check if the deliverer is indeed the right person.

However, it is not necessary to provide the name and the photo of the deliverer to the customers. Since there is no other legitimate ground for this processing, the delivery company is not allowed to provide these personal data to customers.

5.9 Processing operations involving international transfers of HR and other employee data

Employers are increasingly using cloud-based applications and services, such as those designed for the handling of HR-data as well as online office applications. The use of most of these applications will result in the international transfer of data from and concerning employees. As previously outlined in Opinion 08/2001, Art. 25 of the Directive states that transfers of personal data to a third country outside the EU can take place only where that country ensures an adequate level of protection. Whatever the basis, the transfer should satisfy the provisions of the Directive.

It should thus be ensured that these provisions concerning the international transfer of data are complied with. WP29 re-states its previous position that it is preferable to rely on adequate protection rather than the derogations listed in Art. 26 of the DPD; where consent is relied on it must be specific, unambiguous and freely-given. However, it should also be ensured that the data shared outside the EU/EEA, and subsequent access by other entities within the group, remains limited to the minimum necessary for the intended purposes.

6. Conclusions and Recommendations

6.1 Fundamental rights

The contents of communications above, as well as the traffic data relating to those communications, enjoy the same fundamental rights protections as "analogue" communications.

Electronic communications made from business premises may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 paragraph 1 of the European Convention. Based on the current Data Protection Directive employers may only

collect the data for legitimate purposes, with the processing taking place under appropriate conditions (e.g., proportionate and necessary, for a real and present interest, in a lawful, articulated and transparent manner), with a legal basis for the processing of personal data collected from or generated through electronic communications.

The fact that an employer has the ownership of the electronic means does not rule out the right of employees to secrecy of their communications, related location data and correspondence. The tracking of the location of employees through their self-owned or company issued devices should be limited to where it is strictly necessary for a legitimate

purpose. Certainly, in the case of Bring Your Own Device it is important that employees are given the opportunity to shield their private communications from any work-related monitoring.

6.2 Consent; legitimate interest

Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer.

The legitimate interest of employers can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity. A proportionality test should be conducted prior to the deployment of any monitoring tool to consider whether all data are necessary, whether this processing outweighs the general privacy rights that employees also have in the workplace and what measures must be taken to ensure that infringements on the right to private life and the right to secrecy of communications are limited to the minimum necessary.

6.3 Transparency

Effective communication should be provided to employees concerning any monitoring that takes place, the purposes for this monitoring and the circumstances, as well as possibilities for employees to prevent their data being captured by monitoring technologies. Policies and rules concerning legitimate monitoring must be clear and readily accessible. The Working Party recommends involving a representative sample of employees in the creation and evaluation of such rules and policies as most monitoring has the potential to infringe on the private lives of employees.

6.4 Proportionality and data minimisation

Data processing at work must be a proportionate response to the risks faced by an employer. For example, internet misuse can be detected without the necessity of analysing website content. If misuse can be prevented (e.g., by using web filters) the employer has no general right to monitor.

Further, a blanket ban on communication for personal reasons is impractical and enforcement may require a level of monitoring that may be disproportionate. Prevention should be given much more weight than detection--the interests of the employer are better

served by preventing internet misuse through technical means than by expending resources in detecting misuse.

The information registered from the ongoing monitoring, as well as the information that is shown to the employer, should be minimized as much as possible. Employees should have the possibility to temporarily shut off location tracking, if justified by the circumstances. Solutions that for example track vehicles can be designed to register the position data without presenting it to the employer.

Employers must take the principle of data minimisation into account when deciding on the deployment of new technologies. The information should be stored for the minimum amount of time needed with a retention period specified. Whenever information is no longer needed it should be deleted.

6.5 Cloud services, online applications and international transfers

Where employees are expected to use online applications which process personal data (such as online office applications), employers should consider enabling employees to designate certain private spaces to which the employer may not gain access under any circumstances, such as a private mail or document folder.

The use of most applications in the cloud will result in the international transfer of employee data. It should be ensured that personal data transferred to a third country outside the EU takes place only where an adequate level of protection is ensured and that the data shared outside the EU/EEA and subsequent access by other entities within the group remains limited to the minimum necessary for the intended purposes.

* * *

Done in Brussels, on 8 June 2017

For the Working Party,
The Chairwoman
Isabelle FALQUE-PIERROTIN

Annex III

Right to data portability

1. ***How can the data controller identify the data subject before answering his request?***

There are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject. Nevertheless, Article 12(2) of the GDPR states that the data controller shall not refuse to act on request of a data subject for exercising his or her rights (including the right to data portability) unless it is processing personal data for a purpose that does not require the identification of a data subject and it can demonstrate that it is not able to identify the data subject. However, as per Article 11(2), in such circumstances the data subject can provide more information to enable his or her identification. Additionally, Article 12(6) provides that where a data controller has reasonable doubts about the identity of a data subject, it can request further information to confirm the data subject's identity. Where a data subject does provide additional information enabling his or her identification, the data controller shall not refuse to act on the request. Where information and data collected online is linked to pseudonyms or unique identifiers, data controllers can implement appropriate procedures enabling an individual to make a data portability request and receive the data relating to him or her. In any case, data controllers must implement an authentication procedure in order to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR.

In many cases, such authentication procedures are already in place. For example, usernames and passwords, including unique generated codes on mobile devices, are often used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals choose to use without revealing their full name and identity.

If the size of data requested by the data subject makes transmission via the internet problematic, rather than potentially allowing for an extended time period of a maximum of three months to comply with the request, the data controller may also need to consider alternative means of providing the data such as using streaming or saving to a CD, DVD or other physical media or allowing for the personal data to be transmitted directly to another data controller (as per Article 20(2) of the GDPR where technically feasible).

2. ***What is the expected data format?***

The GDPR places requirements on data controllers to **provide the personal data requested by the individual in a format which supports re-use**. Specifically, Article 20(1) of the GDPR states that the personal data must be provided "*in a structured, commonly used and machine-readable format".* Recital 68 provides a further clarification that this format should be *interoperable*, a term that is defined in the EU [23]as:

[23] Article 2 of Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009, p. 20

"the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems."

The terms "structured", "commonly used" and "machine-readable" are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. In that way, "structured, commonly used and machine readable" are specifications for the means, whereas interoperability is the desired outcome.

Recital 21 of the Directive 2013/37/EU defines "machine readable" as:

"a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats."

Given the wide range of potential data types that could be processed by a data controller, the GDPR does not impose specific recommendations on the format of the personal data to be provided. The most appropriate format will differ across sectors and adequate formats may already exist, but the format chosen should be interpretable. Formats that are subject to costly licensing constraints would not be considered an adequate approach.

Recital 68 clarifies that "*The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.*" **Thus, portability aims to produce interoperable systems, not compatible systems.** ISO/IEC 2382-01 defines interoperability as follows: "*The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units*."

Personal data are expected to be provided in formats, which have a high level of abstraction. As such, data portability implies an additional layer of data processing by data controllers, in order to extract data from the platform and filter out personal data outside the scope of portability (such as user passwords, payment data, biometric patterns, etc.). This additional data processing will be considered as an accessory to the main data processing, since it is not performed to achieve a new purpose defined by the data controller.

Data controllers should provide as many metadata with the data as possible at the best possible level of granularity, which preserves the precise meaning of exchanged information. As an example, providing an individual with .pdf versions of an email inbox would not be sufficiently structured. E-mail data must be provided in a format which preserves all the meta-data, to allow the effective re-use of the data. As such, when selecting a data format in which to provide the personal data, the data controller should consider how this format would impact or hinder the individual's right to re-use the data. In

cases where a data controller is able to provide choices to the data subject regarding the preferred format of the personal data a clear explanation of the impact of the choice should be provided. However, processing additional meta-data on the only assumption that they might be needed or wanted to answer a data portability request poses no legitimate ground for such processing.

3. **How do you deal with a large or complex personal data collection?**

The GDPR does not explain how to address the challenge of responding where a large data collection, a complex data structure or other technical issues arise, which might create difficulties for data controllers or data subjects.

However, in all cases, it is crucial that the individual is in a position to fully understand the definition, schema and structure of the personal data, which could be provided by the data controller. For instance, data could first be provided in a summarised form using dashboards allowing the data subject to port subsets of the personal data rather than the entire catalogue. The data controller should provide an overview "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" preferably (see Article 12(1)) of the GDPR) in such a way that data subject can use software applications to easily identify, recognize and process specific data from it. One of the ways in which a data controller can answer requests for data portability is by offering an appropriately secured and documented Application Programming Interface (API). This would enable individuals to make requests for their personal data via their own or third-party software or grant permission for others to do so on their behalf (including another data controller) as specified in Article 20(2) of the GDPR. By granting access to data via an API, it may be possible to offer a more sophisticated access system that enables individuals to make subsequent requests for data, either as a full download or as a delta function containing only changes since the last download, without these additional requests being onerous on the data controller.

4. ***How can portable data be secured?***

In general, the data controllers should guarantee the "appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')" according to Article 5(1)(f) of the GDPR.

However, the transmission of personal data to the data subject may also raise some security issues:

As data portability aims to get personal data out of the information system of the data controller, the transmission may become a possible source of risk regarding those data (in particular of data breaches during the transmission). The data controller shall implement all the security measures needed to ensure that personal data is securely transmitted (e.g. by use of encryption) to the right destination (e.g. by use of additional authentication information). Such security measures mustn't be obstructive in nature and must not prevent users from exercising their rights, e.g by imposing additional costs.

5. ***How do you help users in securing the storage of their personal data in their own systems***?

By retrieving their personal data from an online service, there is always also the risk that users may store them in a less secured system than the one provided by the service. The data subject should be made aware of this in order to take steps to protect the information they have received. The data controller could also, as a best practice, recommend appropriate format(s) and encryption measures to help the data subject to achieve this goal.