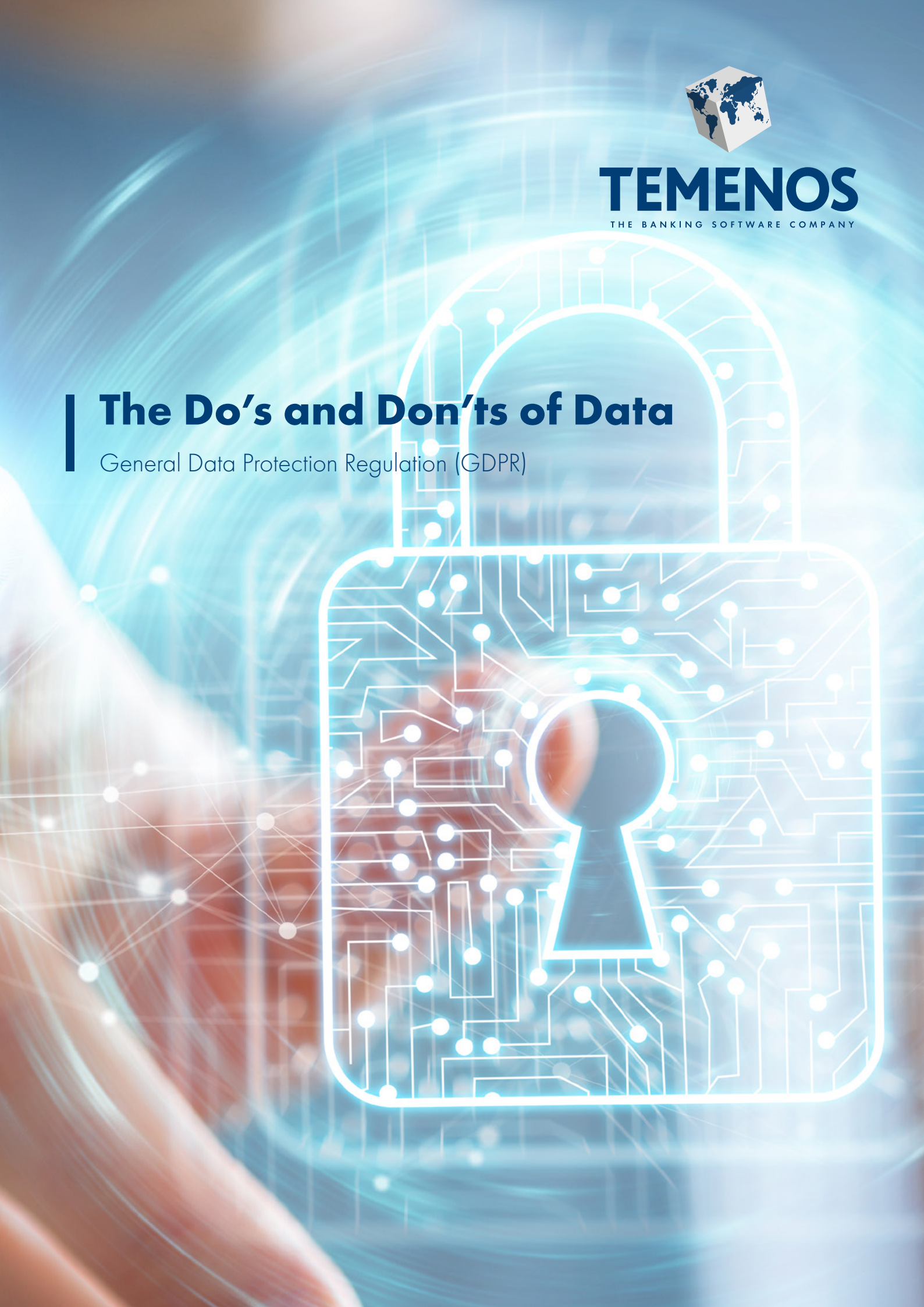
TEMENOS

THE BANKING SOFTWARE COMPANY

The Do's and Don'ts of Data

General Data Protection Regulation (GDPR)



Contents

Introduction

The General Data Protection Regulation (commonly abbreviated to GDPR) is a replacement for the European Union Data Protection Directive which has governed the Protection of Personal Data in the European Union (EU) since 1995.

Since the original directive was passed, there have been a series of rapid technological and business advances which have brought new challenges to the use and protection of personal data. As a result, there was a need for regulators to produce an updated set of obligations to be met by business to reflect the new technological and business landscape.

In addition, the Lisbon Treaty created a new legal basis for a modernised and comprehensive approach to data protection, including the free movement of data within the EU.

The GDPR was designed to resolve three issues that have become apparent with the implementation of the original legislation:

1. There has been an inconsistent approach to the application of data protection across the European Union which has created barriers for business and public authorities due to legal uncertainty and varying enforcement.
2. Difficulties for individuals to stay in control of their personal data.
3. Gaps and inconsistencies in the protection of personal data in the field of police and judicial co-operation in criminal matters.

As part of the free movement of data within the EU, the GDPR gives data subjects (typically EU citizens) a series of enhanced rights in respect to the processing of their data. The cumulative effect of these rights mean to come into effect. that companies need to understand what data they hold and why they hold it. This is important as fines for the most serious data protection breaches will be 4% of worldwide turnover, or €20 million (whichever is higher).

This regulation will require banks to know who in their supply chain receives personal data, where and how it is processed and who has access to the data. This will be an onerous task and banks will need to partner with their technology providers to provide solutions.

Data security will be vital, as any data breach will need to be reported to the regulatory authorities within 72 hours and to inform their customers of any data breach that effects them; resulting in both reputational as well as financial loss.

The key date for the General Data Protection Regulation was 25th May 2018 (after being adopted in early 2016).

One key point to recognise is that to ensure a consistency of approach across the European Union, the GDPR is a Regulation and not a Directive. As it is not a directive, it does not need enabling legislation by national governments to come into effect.

New Data Protection Rights Introduced by GDPR

The Right to be Informed

This means that a customer has a right to know how their personal data will be used. Typically, this will be through a Privacy Notice. This Privacy Notice should be provided free of charge, be transparent and be easy for the customer to access. For any data provided by the customer, the Privacy Notice should include:

- Contact details for the data controller and data protection officer
- Legal basis and purpose for processing
- Data retention period
- A reference to the rights the customer has such as the right to erasure, right to restrict processing, right to data portability, etc.

Such a privacy notice should be made available when someone becomes a customer of the bank with updates provided periodically. The privacy notice should also be available at any time to download.

If there is a personal data breach, Article 34 states that customers should be informed of the data breach if the breach is likely to result in high risk to rights and freedoms of data subjects.

The Right to Access

Under the right of access, the customer can submit a Subject Access Request to access the data held about them. The company holding the data can no longer charge a standard fee for such a request; however, under Article 12 a "reasonable fee" can be charged where the requests are "manifestly unfounded or excessive", particularly if they are repetitive.

The institution holding the data may refuse to comply, but if they do, they must demonstrate why they feel the request is "manifestly unfounded" or excessive in character.

The data that is the subject of a subject access request should normally be provided within 30 days of the request being made; however, this timeline can be extended provided the individual is informed and that the extension has valid reasoning.

The Right to Rectification

An individual has the right to have their data corrected if it is inaccurate or incomplete. If the data has been disclosed to a third party (such as a credit reference agency), they must be informed of the rectification.

The rectification must be done within a month and the customer informed of any third party with whom the data was shared.

The Right of Erasure

The right of erasure is not an absolute right to be forgotten. Individuals have a right to be forgotten and the data to be erased in certain circumstances. For example, a customer's data should be erased when:

- The personal data is no longer required in connection with the reason for which it was originally collected
- The individual withdraws consent to the data being held (and there is no other lawful basis to process the data)
- Where an individual objects to processing and there is no overriding legitimate reason for holding the data
- The personal data was unlawfully processed or it has to be erased to comply with a legal obligation

If the data has been disclosed to a third party (such as a credit reference agency), they must be informed of the erasure of the data.

The request for erasure can be refused if the data needs to be retained to comply with a legal obligation or to exercise defence of legal claims.

For example, when the data of a closed customer must be kept for a time period at the request of the national tax authorities then the data can be kept for that period.

Data retention periods and legal grounds for processing should be established and documented ready for inclusion in privacy notices. So, if personal data is retained for a certain period of time after a customer's account is closed, this should be included in the privacy notice made available to the customer.

> Under the GDPR, bank customers will have the right to receive personal data in a "structured, commonly used and machine readable format" and have the right to transmit their data to another competitor bank without hindrance from the data holding bank.

The Right to Restrict Processing

This is the right of an individual to request a block in the processing of their data. This right is typically temporary and exercised while other investigations are taking place. For example:

- Where an individual has contested the accuracy of the personal data held on them
- Where an individual has objected to the processing and an investigation is taking place as to whether the bank have grounds to override this objection
- Where processing is illegal and the customer has objected to erasure of their data
- Where the personal data is no longer required but the individual requires the data for legal reasons

Typically this would be achieved by blocking the customer and having a standard "blocked for data protection reasons" message. In the KYC data recorded for the customer the, reason for blocking the use of their data would be described in more detail.

The Right to Data Portability

Under the GDPR, bank customers will have the right to receive personal data in a "structured, commonly used and machine readable format" and have the right to transmit their data to another competitor bank without hindrance from the data holding bank.

This doesn't go as far as to require the bank to have compatible systems with competitor banks. The right explains the needs to capture, store and make available data in an interoperable format and enable the bank to respond to such requests. This can be achieved by designing reports containing the required data and allowing the customer to download this data to a machine readable format like a CSV file, or similar.

An example of data portability is the "midata" initiative in the UK where recent transactions can be downloaded and then uploaded to a price comparison website.

If the data is not available for a customer to download immediately, then it should be made available to the customer within a month of receiving the request.

The Right to Object

Under Article 21 of GDPR, an individual has a right to object to their data being used for certain types of processing including:

- Direct marketing (including profiling)
- Processing based on legitimate interests or the performance of a task in the public interest (including profiling)
- Processing for the basis of scientific/historical research

While a data controller cannot refuse to cease processing personal data for direct marketing, it can refuse an objection where there are "compelling legitimate grounds" for the profiling and/or processing being actioned (such as Anti Money Laundering or Sanctions checking).

Details of this right to object needs to be contained in the Privacy Notice communicated to the customer.
Note: The GDPR introduces a new definition of "profiling" (Article 4(4)) which is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements".

Rights Related to Automated Decision Making and Profiling

A customer has the right not to be subject to a decision based solely on automated processing (including profiling) which "significantly affects" the customer or produces legal effects concerning that customer. If a customer contests a decision based on automated decision making and profiling they have the right to human intervention to express their view to contest the decision. For example, if a customer applies for a loan online, and the loan is refused, they have the right to contest this refusal with an employee of the bank.

This right needs to be communicated to the customer in clear language, and the right to withdraw their consent must be clearly defined (therefore if they agree now, they can withdraw consent to this agreement in the future).
In addition, silence and pre-ticked boxes do not signify consent.

This restriction does not apply if the automated decision making is necessary for a contract or expressly authorised by law.

Consent under GDPR

Under the GDPR, consent must be granular and unambiguous. The customer must actively opt into providing consent for certain processing, and silence and pre-ticked boxes no longer signify consent.

Customers must be able to withdraw consent as easily as it is given, and where processing is based on the lawful basis of consent; if the customer withdraws their consent the processing must be stopped and if applicable, the data erased.

Please note: Consent is only one of the lawful basis of processing (the others are Legal, legitimate, Contractual and Vital and Public Interests). If any other of the lawful basis apply, the withdrawal of consent does not necessarily mean processing must be stopped.

Lawful Basis of Data Processing

- Legal
- Legitimate
- Contractual
- Consent
- Vital Interests
- Public Interests

Additional Data Protection Regulations

Data Breach

In the event of a company being subjected to a data breach, Article 33 introduces the requirement to notify regulatory authorities of a data breach within 72 hours. If a longer time period elapses before the data breach is reported, the reason for the delay should be published.

Personal Data

The definition of personal data is widened. The definition contained in Article 4 is "name, identification number, location data, an online identifier, or to one or more factors specific to the physical psychological, genetic, mental, economic, cultural or social identify" of a natural person. So data such as email address, ip address or a collection of indirectly distinguishing data that could be used to identify a person can now be classified as personal data under GDPR.

Geographical Scope

The territorial reach of the GDPR is far more extensive than the previous Data Protection Directive. The new regulation applies to any organisation (including banks and financial institutions) established in the European Union (EU), but also to any which are intentionally offering services to or monitoring behaviours of EU residents if that behaviour occurs within the EU.

The issues related to the transfer of data are addressed in Article 45 of the GDPR, which refers to transfer of data outside of the EU. This would be allowed where the European Commission has decided that the third country protection ensures an adequate level of protection. If the EU Commission has decided that the third country has an adequate level of data protection, then the transfer may not require specific authorisation (subject to any additional regulations applicable to the sector – for example local banking rules).

This means banks and other financial services entities established outside the European Union marketing or selling to consumers within the European Union will need to comply with GDPR. The data subject rights will still apply. Consequently, the same rights to object to processing, to request erasure, etc. would apply, though there is a question over whether or not they could be enforced.

The handling of transfers of data outside of the European Union is largely unchanged, as transfers should only take place if the conditions laid down by the GDPR are met. Transfers are allowed where:

- The European Commission has decided that the third country protection (or a territory or one of more sectors within a territory) ensures an adequate level of protection. If the EU Commission has decided that the third country has an adequate level data protection, then the transfer may not require specific authorisation (subject to any additional regulations applicable to the sector – for example local banking rules)
- Appropriate safeguards are put in place, such as binding corporate rules, data transfer agreements and the EU approved model clauses

Non-EU companies, which are identified to be in scope by the GDPR, will need to appoint a data protection representative within the EU.

Data Protection by Design

Article 25 introduces the concept of "Data Protection by Design and by Default".

> Where processing of data is using new technologies, this may present a risk to individual's privacy. The Bank should carry out an assessment of the impact on the processing/ protection of personal data.

So for example, if a solution was being designed to enable the profiling of customer data, a privacy impact assessment should be conducted. The solution would need to include the ability to exclude customers from the profiling where a customer or number of customers have objected to the profiling.

This is not just an obligation required at the time of technical design but also includes taking into account data protection when designing workflows and defining both project and operational procedures. Under the GDPR, the controller has an obligation to introduce "appropriate technical and operational measures" such as "pseudonymisation" and "data minimisation" to ensure there are the necessary safeguards in place to the rights of the data subjects under the GDPR.

Consequently Data Protection by Design assessments will need to be carried out both during the operational and implementation phases (for example during the process of data migration).

This will include both a Data Protection Impact Assessment as part of any project initiation and an ongoing review of operational procedures to meet the local data protection certification requirements.

Impact on Financial Services Companies

Privacy Notice

As a result of the GDPR, financial services companies will need to supply a significant amount of information to customers whose personal data is held by them including:

- Contact details of the data controller
- Contact details of the Data Protection Officer (if one is appointed)
- The lawful basis for holding the data and whether the data is required by law or as a result of a contract
- If the data is processed based on the customer's consent, the customer should also be alerted to the right to withdraw that consent
- The data retention period
- Details of the customers rights under the GDPR such as rights to erasure, right to object to processing, right to data portability and how to complain to a regulatory authority
- The existence of any automated decision making (including profiling and the right to object to profiling) and how to object to an automated decision
- There are also requirements to inform the customer of whether the data is collected from themselves or a third party

The language used on the Privacy Notice should be transparent and easily accessible.

In advance of the implementation of the GDPR, it is recommended that financial services companies review the content of their Privacy Notices to ensure they are still compatible with the GDPR.

Processing

The grounds for processing must be established, for example: processing is necessary for the performance of a contract which the individual is party to, and details must be provided to the customer under the Privacy Notice. There is a higher threshold for "consent" under the GDPR, which means that the circumstances it is relied upon may be more limited going forward. The lawful grounds for processing should be recorded for compliance purposes and included in the Privacy Notice. When relying on consent, the data controller may want to see what alternative processing condition can be used. If consent is relied upon, the following must be taken into account:

- Where a customer has given consent to their data being processed, that consent must be recorded. Whenever consent is given, the customer must also be given details of their ability to withdraw that consent.
- While consent can be recorded by ticking a box below a consent statement, it should be noted that silence and pre-ticked boxes do not constitute consent.

In addition, any objection from the customer in regards to their data being used for marketing profiling should be recorded. If an objection is received by the bank, then the customer should be flagged as having recorded that objection. If the customer is flagged as objecting to their data being used in profiling, then they should not be included in any direct marketing processing that includes profiling.

If an automated decision is made that impacts the customer, they have the ability to record their objection to the decision and request the decision to be reviewed with human intervention. The customer should have the opportunity to speak to a member of the bank staff to explain why they object to the decision.

Data Portability

The easiest way for a financial services institution to comply with the right of data portability is to provide a customer with the ability to download personal data to an appropriate format (which could be a csv file) from their online channel. Where no online channel is available, this would need to be provided via a branch with appropriate safeguards in place.

This right of data portability could also be viewed as an opportunity, as it would enable customers to easily perform comparisons between competing financial institutions or could be used to help capture new business.

Erasure and Rectification

The right to erasure is often described as the "right to be forgotten". This means that when the data is no longer required, a customer has the right to request that their data is erased. Typically, this will be at the end of the data retention period described in the Privacy Notice; for example, 5 years after the customer has closed their account and ceased business with the bank. There are exceptions to this (typically to comply with legal requirements; for example, if the tax authorities have requested data is retained for a given time period). If a financial services company refuses to comply with a request for erasure, they must give a valid reason why the data cannot be erased.

The customer also has a right to rectification. Obviously, holding correct data is important, so correcting mistakes is a fairly obvious step.

However the right to rectification means that the data must also be rectified on all the databases where it is held and by any third party with which the data has been shared (for example a credit agency). Appropriate supplementary information should be provided by customer's to validate any rectification requests.

Subject Access Requests (SAR)

Most financial services companies will already have procedures to respond to a subject access request from one of their customers; though, these should be reviewed as a customer will be entitled to more information and the response time has reduced to 1 month (from 40 days). However, companies will no longer be able to charge a fee unless the request is unreasonable or repetitive, so a procedure should be put in place to decide what 'unreasonable' means and how much will be charged to respond to any unreasonable request.

Data Accountability

Under the GDPR, data controllers must demonstrate that they are accountable for the data they hold. This includes putting in place appropriate procedural and technological measures to ensure that the company is using personal data in accordance with the GDPR.

Typically, this will be done by using data protection by design principles to design a process where data protection principles are embedded in the processing including:

Recording what data a bank holds and why, so undertaking an assessment of where and how data is collected and stored is vital. Banks should analyse their databases and the technology which transmits/stores data

- The data retention period used
- The accessibility of the data (both to staff and customers) to ensure it is only available to a limited group of people
- Conducting a Privacy Impact Assessment

The documentation recording the data protection design should be available to the regulatory authorities if required to prove appropriate measures to prevent data breaches have been enforced.

Some of the measures suggested when designing data protection at either a technological or procedural level includes:

- Keeping a record of all data processing is vital to ensure accountability, as this will be onerous working with technology suppliers will be required
- Pseudonymisation and encryption of personal data
- The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services
- A process for regularly testing and evaluating data security measures

In this regard, "pseudonymisation" is defined as a way of processing data in such a way that the data subject can no longer be attributed to a specific data subject.

Data Protection Officer

The appointment of a Data Protection Officer (DPO) is not mandatory; however, it is required if:

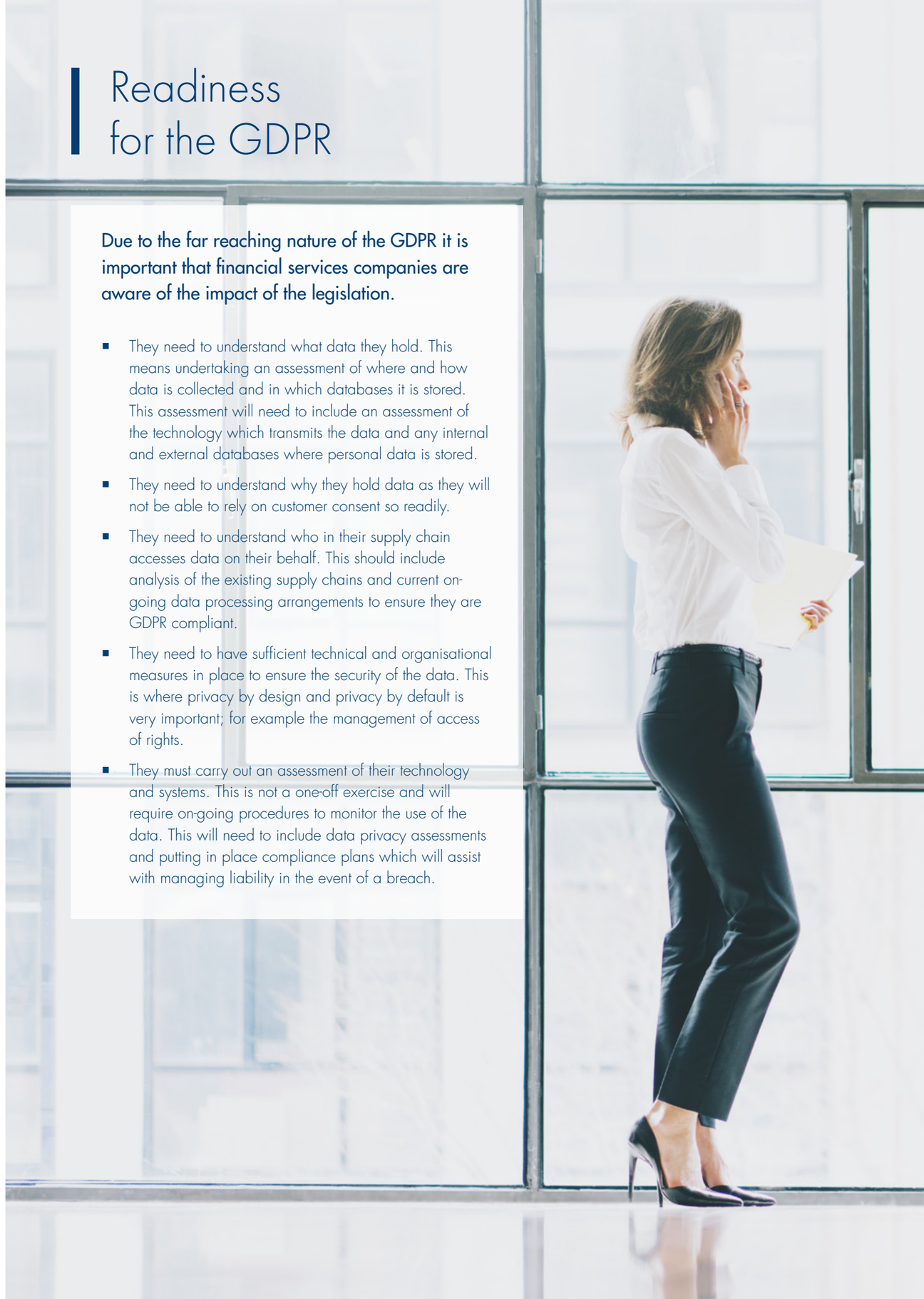
- The core activities of the processor consist of operations which require regular and systematic monitoring of data subjects on a large scale
- The activities involve large scale processing of sensitive data (data such as their racial or ethnic identify, religious beliefs, sexual orientation, etc.)

Many large financial services firms already have Data Protection Officers in place, but under the GDPR, the DPO should be independent of the data controller and report directly to the highest level of management. They should not be penalised for carrying out their tasks, particularly in highlighting and data protection concerns or breaches to the most senior management of the bank.

Readiness for the GDPR

Due to the far reaching nature of the GDPR it is important that financial services companies are aware of the impact of the legislation.

- They need to understand what data they hold. This means undertaking an assessment of where and how data is collected and in which databases it is stored. This assessment will need to include an assessment of the technology which transmits the data and any internal and external databases where personal data is stored.
- They need to understand why they hold data as they will not be able to rely on customer consent so readily.
- They need to understand who in their supply chain accesses data on their behalf. This should include analysis of the existing supply chains and current on-going data processing arrangements to ensure they are GDPR compliant.
- They need to have sufficient technical and organisational measures in place to ensure the security of the data. This is where privacy by design and privacy by default is very important; for example the management of access of rights.
- They must carry out an assessment of their technology and systems. This is not a one-off exercise and will require on-going procedures to monitor the use of the data. This will need to include data privacy assessments and putting in place compliance plans which will assist with managing liability in the event of a breach.



temenos.com

Temenos AG (SIX: TEMN), headquartered in Geneva, is the world's leader in banking software, partnering with banks and other financial institutions to transform their businesses and stay ahead of a changing marketplace. Over 3,000 firms across the globe, including 41 of the top 50 banks, rely on Temenos to process both the daily transactions and client interactions of more than 500 million banking customers. Temenos offers cloud-native, cloud-agnostic front office and core banking, payments, fund management and wealth management software products enabling banks to deliver consistent, frictionless customer journeys and gain operational excellence. Temenos customers are proven to be more profitable than their peers: over a seven-year period, they enjoyed on average a 31% higher return on assets, a 36% higher return on equity and an 8.6 percentage point lower cost/income ratio than banks running legacy applications.
For more information please visit www.temenos.com.

©2017 Temenos Headquarters SA - all rights reserved. Warning: This document is protected by copyright law and international treaties. Unauthorised reproduction of this document, or any portion of it, may result in severe and criminal penalties, and will be prosecuted to the maximum extent possible under law.

TEMENOS

THE BANKING SOFTWARE COMPANY