THE TA FORUM

General Data Protection Regulation (GDPR)

Best Practice Guidance

This Best Practice ('BP') Guidance note looks at the key impacts and challenges to Transfer Agents ('TA's') in respect of the General Data Protection Regulation ('GDPR') and the proposed solution to these challenges based upon feedback received from member firms of the TA Forum. It is the regulated firms responsibility to ensure compliance of GDPR, which comes into effect in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Who does the GDPR apply to?

•The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the Data Protection Act (DPA) – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

•The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

•The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

There is however one key change in the GDPR definitions compared to the previous regime. The criteria which define the difference between controller and processor have been altered and are now based on the activities undertaken and the level of discretion to which the firm carrrying on these activities has. Critically the new defintions introduce the potential for both the product provider and the TA (if they are different legal entities) to be data controllers (termed co-controllers).

What information does the GDPR apply to?

Personal data

Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. It can be assumed that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Given one of the main objectives of GDPR is to ensure data protection legislation keeps up with technological developments, the definition of personal data now explicity covers any information which can be linked to an individual, such as ip addresses and information linked to those forms of identifiers.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data". These categories are broadly the same as those in the DPA, but there are some minor changes.

For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Areas of focus for TA's:-

Systems – where is personal data stored and where does it flow to

- Systems upgrade maybe required to incorporate the Data removal functionality.
- A Data inventory is required to enable articulation of where Data is held and how it flows through IT architecture.
- Corresponding business processes and flows will need to be updated to facilitate accurate monitoring of data in and out of the business and facilitate Privacy Impact Assesments (PIA's).
- Once system/process has been established, ongoing maintenance will be required ensuring that an owner and process for it's upkeep is identified.

Upgrade existing Data Protection Policies – to include handling of new investor rights and breach reporting .

- Ensure process encapsulates how to provide clients with a clear and concise overview of how data is processed, managed and protected.

Clearly define Data Retention, Dissemination & Destruction Policy Policies – for adequate retention and minimisation of data, alongside controls for the ongoing handling

- Review of existing control framework surrounding the handling of personal data including when the data is required to be sent externally eg to another area within a firm, to a vendor, to a client, to a Regulator/Tax Authority etc.
- Retention and Destruction Policy should explicitly document and review any exceptions. The purpose being to ensure that the policy is robust, easy to implement and easy to understand and follow and ensure that all exceptions are valid, visible and managed.

Client Company/Third party/Vendors contracts

- 3rd party TA's should establish whether they will be defined as data processors, data controllers or co-controllers under their current contractual terms and scope of services.
- Data Controllers and Processors have a responsibility to ensure that Third Parties that process client data on their behalf do so in accordance with their own policies and that where the TA is the Data Processor that robust data protection management and security in line with the regulatory obligations is provided.
- All existing and future contractual relationships to be reviewed to ensure firms remain compliant with Data Protection legislation.

Employee and client training

- Employee training is significant. TA's are looking to facilitate customer engagement via online journeys and call centre scripts.

Current Challenges/Issues and proposed best practice:-

Right to be forgotten v data minimisation requirements

- It is understood that where personal data is held which is not 'necessary' or no longer 'necessary' for the purposes for which it was obtained - this can be challenged and the Data Subject can request that it is deleted. (i.e. data held must be 'adequate, relevant and necessary'). However we believe there is significant confusion across the financial services industry as to the extent to which this is likely to impact.

- The 'Right to be Forgotten' is intended to explicitly target tech companies, where incorrect or in extreme cases slanderous/libellous information can exist in perpetuity. While this can of course impact TA's it should be noted that such a right is not automatic and is subject to and does not supersede other regulatory obligations. In reality while a customer can request, it is very difficult to ascertain under what circumstances such a request would be legitimate (unless the investment was set up fraudulently but even then such data could not be deleted because of the legal considerations) and our thinking in this area would be to advise that the customer close/sell any/all open positions/investments and that subject to the Data Retention Policy, their data would then be deleted.

- In respect of Data Minimisation this targets companies that typically 'harvest' data that is not required for the purposes for which it is was obtained and then using or selling such data. Data Privacy Policies and PIA assessments should ensure that superflous information about investors is not gathered.

- The legal basis for processing the personal data and an internal record retention policy linked to other regulatory requirements eg 4th AML, MiFID II etc mean a potential rejection and non-applicability for right to be forgotten requests.

Volume of unstructured data held within TA – Outlook, Excel, SharePoint etc. How to detect and remove?

- An audit to ascertain the magnitude of the data held should be undertaken, to include both operational and non-operational areas. This should also identify the types and nature of data held, (e.g. internal reports, copy letters etc.), and rationale together with the control measures that are in place to restrict access.

- True exceptions should be logged as such as part of the businesses data retention policy. Where no valid exception is identified the data should be removed/deleted and alternative processed/systems/procedures implemented that are compliant.

- A corporate file structure should be implemented and linked to the record retention policy. An automatic corporate archiving solution should be considered which sweeps the associated drives and deletes records once their associated retention period expires.

Jurisdictional data retention requirements applicable to cross border products

- Programme structure should provide oversight and ability to identify risk. This is a challenge as different record retention periods exist per jurisdiction (Ireland, Luxembourg & UK considered) where there is little appetite to align these periods.

Deletion of data v anonymisation

- The ICO recognizes that 'Data' deletion is often not possible in operational systems without significant cost and complexity and in response offers the alternative of **putting information 'beyond use'**[1].

- The ICO will be satisfied that information has been 'put beyond use', if not actually deleted, provided that the data controller holding it:-

    - is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
    - does not give any other organisation access to the personal data;
    - surrounds the personal data with appropriate technical and organisational security; and
    - Commits to permanent deletion of the information if, or when, this becomes possible.

- The ICO states that it will not require data controllers to grant individuals subject access to the personal data provided that all four safeguards above are in place. Significantly the ICO currently states it will not take any action over compliance with the fifth data protection principle.

- In respect of the above there are generally considered to be two alternatives to Deletion:

    - **Data Anonymisation** is a valuable tool that allows data to be processed/stored/retained, whilst preserving privacy. The process of anonymising data requires that identifiers are irrevocably changed in some way such as being removed, substituted, distorted, generalised or aggregated. This allows companies to effectively preserve the relational integrity of their databases while at the same time making it extremely difficult to 're-identify' a customer or an investor. Anonymisation is in many respects akin to deletion.

    - **Data Pseudonymisation** refers to the technique of processing/storing/retaining personal data in such a way that it can no longer be attributed to a specific "data subject" without the use of additional information (data keys etc.), which must be kept separately and be subject to technical and organisational measures to ensure non-attribution. Like Anonymisation this approach allows companies to effectively preserve the relational integrity of their databases while at the same time making it extremely difficult to 're-identify' a customer or an investor. However, it is not considered as secure as full Anonymisation.

- This is in line with the ICO Guidance* which can be accessed from the website below which recognises that a 'hard' delete is not necessarily practical or viable.

[1] Guidance can be accessed here: https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

However it is important for firms to be aware that undertaking a strategy of data anonymisation / pseudonymisation introduces a new specific risk to the firm under the new regime. Reversing anonymised data or providing the means by which an employee or associated party can reverse engineer scrambled/anonymised data is proposed to be a criminal offence in the UK.

Volume of personal data held and managed by vendors

- Where customers data is passed to a 3rd party vendor, the event would be identified by Data Gov & Process analysis.
- Some TA's have a workstream dedicated to 3rd party contracts who will apply any revisions for specific data usage.
- Existing legal contracts with vendors should include provisions regarding processing personal data (data held is viewed as processing).

Determine legal basis for processing personal data – avoid consent where possible

- Legal basis for processing personal data is based on the 'contract' between the investor and the TA client via the signed application form/T&C's i.e. not based on consent, therefore providing that when on boarding a new customer they are made aware of the firms Data Processing Policies and their rights therein in a clear and unambiguous manner that such considerations need not be onerous.

- In respect of the revocation of consent we see this in much the same way functionally as the right to be forgotten and our thinking in this area would be to advise that the customer close/sell any/all open positions/investments and that subject to the Data Retention Policy, their data would then be deleted.

- Consent for processing may however need to be obtained for information collated for marketing purposes. Online journeys will need to be changed to implement a robust and consistent approach to capturing consent across all channels.

Breaches to be notified to supervisory authorities within 72 hours

- Currently considerations include a dedicated DPO and supporting Data Governance Team be implemented to ensure adherence to the regulations and provided adequate support and policing of new processes and procedures.

- Ensure programme to include process enhancements to the data capture of a Breach Event and automate regulatory reports for the purposes of the 72 hr deadline.

Privacy Impact Assessments required – new systems and high risk processes

- PIAs to be introduced as part of the Data Governance work stream of the GDPR Program. This will introduce a PIA process and template as a deliverable in the Project Lifecycle and will put 'Privacy by Design' at the forefront of change management processes.

Enhancements to Data Governance Frameworks – DPO, policies & procedures, training – corporate level v TA/business unit

- A new DPO operating model to be implemented as part of the GDPR programme.

Employees are the weakest link to the security of data

- Member firms already have in place mandatory training with respect to security of all data. There will be new and amended business processes introduced to ensure compliance with GDPR.

- The processes and procedures will be documented and training provided including a review of the annual mandatory training materials.

Additional issues/challenges under consideration:-

- Consider whether contact and signatory lists for institutional clients are caught by GDPR and therefore will need to review how they are stored and updated.
- Subject Access Requests - potential increase in the number of requests received, process required to be able to extract all information held, query as to whether this extends to extracting telephone calls

Important Information

This document has been compiled for the use of TA Forum members only and is for guidance purposes and has been written from the view point of TA's and the administration activities that they perform for regulated firms. Where any firms require further clarification of the rules, guidance should be sought from the FCA. It is the regulated firm's responsibility to comply with the regulatory rules and ensure that they receive all required information in order that they can perform adequate oversight regularly.

*Source: https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/