

CASE STUDY



macro global[®]
creating value through innovation

Brexit & GDPR Compliance – The door to the future



Executive Summary

” Gaining and maintaining the trust of your customers is crucial if you ever want to grow your business, that’s a tough sell.”

From 25th May 2018, the General Data Protection Regulation (GDPR) took weight as a leash on shoulders for the organisations processing and withholding data transfers subject to the post-Brexit. As we speak during the transition period which is perpetual with new regulations across demographics with dooms and glooms.

In this case study, we will discuss about the numerous shades of grey that our clients were trying to address their state of business and operation post-Brexit. So, let's get a perspective clear that any financial institutions established in the UK offering service to the EU region post-Brexit must **comply with both the UK legislation and the EU-GDPR** which needs highlighting.

No-Deal Brexit & GDPR Outlook

To a certain degree during the current Brexit transition period, the opt-in to no-deal Brexit by the UK has made the near future tangled the GDPR Outlook which affects the data protection rules that impact the data transfers on small and medium-sized business and organisations between EU and UK. Post-Brexit UK being regarded as a third country, businesses and organisations that process personal data should continue to follow the existing guidance for advice on their data protection obligations. EU law will continue to apply in the UK, including the EU General Data Protection Regulation (GDPR), after which the GDPR will be converted into UK law.

Business Challenge Two-Edged Sword

The biggest area of data privacy that Brexit will affect is data transfers. Personal data can currently move freely around the European Economic Area (“EEA”), yet this free movement of personal data to a country outside the EEA (i.e. a “third country”) is not permitted, and any such transfer of personal data is known as an “international transfer”. Post-Brexit UK will be a third country for the purpose of international transfers, so if an organisation based in the EEA wishes to transfer personal data to an organisation based in the UK, they have to ensure there is a transfer mechanism in place. Given that the UK GDPR mirrors the EU's GDPR, transferring data from the UK to third countries remain available.

Irrespective of the political situation in the UK, all financial institutions should continue to make sure they comply with the GDPR as it currently applies following DPA 2018 act which would be converted into UK GDPR post-Brexit. Organisations should identify the existing relationships with vendors, involving the transfer of personal data.

In the event of a no-deal Brexit, the government has advised organisations to prepare accordingly to ensure any transfer of EU citizens' personal data to the UK is indeed compliant with privacy laws. Hence, UK based financial organisations should review their data flows and make necessary amendments to all contracts with vendors that involve the transfer of personal data. The most common problem faced by the majority of UK-based financial institutions is that they already possess personal data and the consequences may be devastating for organisations if they do not fully understand the new guidelines and utilise the customer data in a lawful manner.

GDPR – Adequacy Decision

Adequacy is a status granted by the European Commission to a non-EEA country in which they confirm the level of personal data protection provided by that country is essentially of an equivalent level to that of EU Member States. If the UK is awarded 'adequacy', data flows from the EU to the UK will continue to flow freely until 2021.

In the absence of an adequacy decision, it may still be possible for the UK to negotiate a Privacy-Shield type arrangement, similar to the EU-US Privacy Shield. If there's a failure to agree on any data protection arrangements, UK organisations which receive personal data from the EU (and EU organisations transferring data to the UK) need to ensure they have additional appropriate safeguards in place. For example, Standard Contractual Clauses or Binding Corporate Rules. To continue receiving data from the EEA, organisations need to review their contracts and enter into special agreements with European customers, and other business associates.

One of the spotlights of the General Data Protection Regulation (GDPR) is the facilitation of the free flow of data between EU member states. In order to smoothen the progress of international transfers of personal data, the GDPR sets out various transfer mechanisms. One of these is an "adequacy decision," i.e. where the European Commission has decided that the third country (the UK) ensures an "adequate level of data protection." This presents a compliance risk for UK-based organisations in particular as they would need to have a legal mechanism in place for demonstrating adequate data protection. In accordance, there are a limited number of legal mechanisms that organisations can turn to provide adequate protection for data when transferring it outside of the EEA. The flow of data is abundant for many businesses due to the international provision of services and operations across markets. This will have a major impact on any organisation that routinely transfers personal data from the EU to the UK (including UK-based organisations providing services to customers in the EU).

Sharing the personal data of customers is vital to the legitimate operation for any business. However, it is important for financial institutions to take steps to ensure and continue to transfer data after Brexit (particularly a no-deal Brexit) without any interruption to your business. Although the GDPR is a piece of EU law, businesses which continue to work with companies and individuals in the EU will need to comply regardless of the data protection laws in the UK. For example, if you are an organisation collecting the personal details of customers in the EEA, you will need a special agreement to comply with data protection laws.

Beginning the transformation – Roll the dice

In today's data-rich business environment, financial services firms have an opportunity to get hold of GDPR. Through a comprehensive framework, and data protection controls and processes, Macro Global create more transparent, trust-based relationships with clients. We apply a common set of personal data management principles to all clients, providing a framework for processing personal data in compliance with GDPR, local privacy laws, and professional standards as well as their own internal policies.

What we did – The known unknowns

Our client who is a foreign bank in the UK accompanied by nearly 2,50,000 clients requires a strong security system to protect their business operations in all aspects as they transfer personal information of their customers for the SCV Auditing drive to comply with FSCS Regulatory reporting. In an era of post-Brexit, they require to remain vigilant and being cognisant of having controls in place wherever necessary to protect their customer data under PIP and comply with data transfer rules. Personal and sensitive data information is moved into the cloud or on-premises repositories with increased data volume. Hence, the client demands greater data protection governance to ensure responsible access and usage that maintains trust.

Macro Global's team processes are stringent over the security norms that need to be addressed within our scope of service agreement and solution to meet our clients' unique data protection expectations. Data protection security governance is implemented across "SCV Forza – FSCS SCV Automation Platform" and "SCV Alliance – FSCS SCV Audit Platform" solution to ensure as we deal with customer personal information. Macro Global's service on data protection benefits organisations improve data privacy, meet compliance goals both (Pre & Post-Brexit) including Deal/No-Deal, and build an environment that the customer data is safe and protected.

GDPR compliance is succeeded through a consistent framework approach by:

Governance

- Defining and roll out a robust governance model to implement data privacy programs engaging with clients.
- Defining regulated data policies, and align across people, processes, and systems.
- Re-define data governance policy framework, data principles, and integrate them within existing functions.
- Internal client dependent Audit Data Monitoring SPOC.
- Design and develop privacy impact assessments.
- Review and update Client Contracts for data privacy clauses.
- Conduct privacy assessments regularly and as and when new product processes are launched.

Operations

- Subject matter experts implement and monitor best practices and regularly review the effectiveness of security processes and controls.
- Protect personal data and comply with privacy regulations and corporate standards.
- Define processes for recording consent, correction of stored data, data erasure, and portability.
- Security controls to protect client data when accessed, handled, transmitted, hosted, or stored.
- Define a policy for retention and disposal of data.
- Integrate security solutions with regular operations.
- Establish data audit trails.
- Maintain system activity report logs, templates, response records of data subjects.
- Maintain incident logs and conduct regular compliance, audit, and vulnerability tests.

Macro Global's Deal on GDPR

“GDPR has been an important regulatory force for mobilising data protection efforts. However, it is not the end of the road.”

Financial firms face the task of reaching regulatory compliance in the short term while preparing themselves for the data protection requirements of the future. When working with customer data, it is crucial to ensure regulatory compliance and security in the cloud and on-premises. Macro Global partnered with Microsoft to support the security architecture, product implementation of its both "SCV Forza - FSCS SCV Automation Platform" and "SCV Alliance - FSCS SCV Audit Platform" solution to ensure that the environment is highly secured. Macro Global looks ahead in recognising the underlying technology to remain competitive in a financial ecosystem by managing and achieving the GDPR compliance post-Brexit through below technical controls.

Identity and Access Management (IDAM)

Having proper IDAM controls in place help limit access to personal data for authorised users and ensure that users have access only to information or systems applicable to their job function.



Incident Response Plan (IRP)



IRP addresses the phases such as preparation, identification, and control. An incident response plan and a disaster recovery plan in place help to mitigate risk and prepare for a range of events.

Policy Management

To be effective, organisational policy acknowledgement and training ensure policies are properly communicated and understood. Put it all together and followed accordingly, policy management is a foundation for compliance toward GDPR readiness. Supporting standards and controls are continually vetted by senior management to confirm that the material remains timely and accurate and that it correlates to legal and regulatory requirements.



Security Certification Process



Prior to implementation, all applications and systems subject to the security certification process to confirm that they have been developed in accordance with security policies and secure application development standards. The security certification process incorporates risk assessment and vulnerability assessments and maintains the confidentiality, integrity, and availability of Macro Global information and that of Macro Global clients.

Data Loss Prevention (DLP)

Relevant to GDPR, DLP helps prevent the loss of personal data. Organisations, whether they are the controller or processor of personal information, are held liable for the loss of any personal data they collect. Incorporating DLP controls adds a layer of protection by restricting the transmission of personal data outside the network.








Data Residency and Retention



MG engaged with Azure services enable the customers to specify the region into which the service must be deployed and thus control where the customer data must be stored. In addition, in the event of an outage affecting multiple regions, at least one region in each geolocation will be prioritised for recovery. This provides resiliency and business continuity. Data governance have been implemented over cloud infrastructure and on-premises, including but not limited to which services can be deployed, resource monitoring requirements, or regions in which resources can be organised.

Below measures are followed to meet the requirements

-  Establish governance structure – a team with representation from business lines, IT security, legal or compliance.
-  Define all the policies and rules on sensitive data elements – where the data need to be located, what needs to be encrypted.
-  Reports to monitor the application of policies; measure how much data resides and identify deviations.
-  Tools to track the source of information and how it gets processed and transformed.
-  Review the data held on the system to decide whether to destroy or delete the data once the purpose it was created is no longer relevant.

Our Success Story – Following Footprints

Macro Global secures the information assets of Macro Global clients through the adherence to the data protection and security controls. We understand the importance of taking appropriate steps in safeguarding information and are committed to protect the information of our clients.



Subject the systems to both data privacy impact assessments and security certification reviews, which support a robust, consistent approach in deployment and operation.



We protect personal data within the network using appropriate physical, technical and organisational security measures.



Practices and controls to confirm that your data is managed properly and securely, in accordance with legal and regulatory requirements.



Continuously remediate data privacy risk with predefined policies for risk analysis and prevent unauthorised data use and access violations.

We are here to help you

If you want to learn more about our products or services or just have a question?

If you need advice from our expert team who understand your business better than our peers?

If you want to know how we transformed businesses using our unparalleled industry and domain expertise?

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

<https://www.macroglobal.co.uk/contact-us/>

