SICSIC ADVISORY
FINANCIAL SERVICES RISK & REGULATION

CLIENT BRIEFING NOTE

Data Protection for UK insurance post-Brexit

February 2021

Little changed overnight for data controllers when the UK left the EU and the transition period ended on 31 December 2020. The Trade and Cooperation Agreement provided a grace period of up to six months during which time personal data can continue to flow freely from the EEA to the UK. The European Commission has since published a draft decision which states that the EU considers the UK's data protection regime as adequate. Although this is a draft decision, if approved then it proposes that the decision will be valid for four years from the date that it is formally ratified, assuming that the decision remains unchallenged during that time.

However, this isn't the only consideration for firms when it comes to data protection. Brexit has impacted other aspects of GDPR, and it is more important than ever for financial services firms to understand any new exposures the changes will bring, and update their approach to GDPR compliance accordingly.

Whilst an adequacy decision means that data can continue to flow freely from the EEA, there are other considerations for organisations when managing data protection rules in a post-Brexit UK.

What remained the same?

The principles of GDPR and the rights of individuals haven't changed. UK firms will continue to have a requirement to comply with the following local regulations in relation to processing of personal data belonging to UK individuals including its customers, contacts and employees:

- *Data Protection Laws and Regulations including the UK General Data Protection Regulations (UK GDPR);*
- *Data Protection Act 2018; and*
- *Privacy and Electronic Communications (EC Directive) Regulation 2003 (PECR).*

However, where data was processed relating to EEA individuals prior to 31st December 2020, the EU GDPR as it stood on that date will continue to apply to that data (known as frozen GDPR). Additionally, any new personal data collected and processed in respect of EEA citizens from 1 January 2021 will be subject to the EU GDPR including any subsequent changes or amendments to that regulation.

What changed?

What happens to transfer of personal data from the UK to the EEA?	Under the UK GDPR you can continue to transfer UK personal data to the EEA.
What about transferring personal data from the UK to Non-EEA countries?	You should already have additional safeguards in place to transfer data outside of the EEA. This can be an adequacy decision under the EU (which the UK will still rely on) Existing Standard Contract Clauses (you may need to amend these to reflect the UK rather than EU GDPR) or other measures in the same way as you were required to do under the EU GDPR.
What about non-EEA – UK transfers?	This hasn't changed for now. The UK continues to work with non-EEA countries to make arrangements for transfers to the UK. The sender will need to comply with the rules in their country. Existing EU Adequacy Decisions will be recognised by the UK and existing standard contract clauses will be recognised but may need to be updated.
Can I continue to offer goods and services to customers in the EEA?	Yes. You will need to comply with both the UK and EU GDPR. You need to be able to easily identify and separate where data comes from and who it belongs to. As time goes on these rules may change and you'll need to understand which version applies to which data.
Do I need to appoint an EU representative?	If offering goods or services to EU individuals, UK companies will need an EU representative. If no office in the EU they will need to appoint a representative in the country where they most commonly offer goods or services. There are exemptions for this where the processing is "occasional, does not include, on a large scale, processing of specialist categories of data". The Article 29 Working Party took the position that activity can only be considered "occasional" if it is not carried out regularly and occurs **outside the regular course of business** or activity of the controller or processor.
Applicable rules	The UK GDPR, Data Protection Act 2018 and PECR will continue to apply in respect of UK Data. EU GDPR and privacy regulations will apply to EEA Data, local data protection laws will apply to areas outside of the EEA as before.
What happens to cross border processing?	Cross border processing is between EEA states only. You will no longer be carrying out cross border processing from the UK, although this can still be the case between your EEA establishments. The UK will no longer benefit from the "One Stop Shop" and so: • If you have one establishment in the UK and one in the EEA, you need to be registered with both supervisory authorities and action can be taken by each. • If you have more than one EEA establishment, you would register with the ICO and EEA Supervisory Authority where you have the larger base and they will become the Lead EEA Supervisory Authority, again action could be taken by both. • If you have no establishment in the EEA and have a data breach, action could be taken by all supervisory authorities in the areas affected.

Contact

Sicsic Advisory can provide you with guidance and support to update your GDPR policy frameworks, training and awareness delivery and process alignment to ensure a continued compliance with the regulations whatever the outcome.

Michael Sicsic
Managing Director
michael@sicsicadvisory.com

Sandra McGreechan
Senior Consultant -
Data Protection Expert
sandramcgreechan@
sicsicadvisory.com

References:

- The Trade and Cooperation Agreement
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
- ICO Guidance
- Data protection: draft UK adequacy decision

Implications for the UK insurance industry

When an insurance broking firm is operating in the UK with customers, data processors, contacts or employees in the EEA, the decision on adequacy will be an important factor in keeping data flowing. Now that they are no longer in the EU, there are other implications and risks that the draft decision on adequacy doesn't change. This includes the very real exposure and risk that firms could potentially be subject to, such as an action from multiple supervisory authorities as a result of one incident, now that the "One Stop Shop" no longer applies to regulatory supervision.

When you need to consider the next steps – real life challenges for insurers and brokers

What happens to existing group policies written under GDPR rules where a new claim is submitted by an underlying EEA policyholder (possibly previously unknown to the insurer) containing sensitive/ personal information and the policy has been retained by the UK insurer?

A broker receives a claim containing sensitive information from a policyholder in the EEA. Even though the policy has been retained by the UK insurer, they will now be processing personal data belonging to an EEA citizen. Brokers will be establishing a new activity as a result of logging and managing the new claim and processing data of that individual for the first time; the EU GDPR and any subsequent amendments will apply to the new personal data processed. Where there is no establishment in the EU, brokers will need to inform the individual who their EU Representative is (for example in a privacy notice).

Understanding all the contractual parties involved: what has changed post-Brexit, what data is now held by whom, how will firms ensure that future data being shared is done so with the correct parties under the right regime?

Brokers need to understand all the contractual parties involved, how data flows now and consider how it will need to flow in the future to be certain that the appropriate agreements are in place and identify which rules apply to which processes. The key to managing this going forward is to review current information audits and Records of Processing Activities and identifying the current position in relation to data flows. It will also be important to review all Data Processors and any current data sharing agreements and contracts and understand where the need arises to create new agreements between parties.

A UK broker with a UK commercial client deals solely in the UK, but the firm has a subsidiary based in Spain insured under a global policy with an insurer who is EU and UK authorised to write such business. Do you as the broker have any exposure to any data they obtain in respect of the Spanish subsidiary?

The UK broker still has a responsibility to manage any personal data in accordance with the relevant regulation. In this case, where they collect, process or store any personal data relating to a contact within the Spanish subsidiary. However, it's important to establish whether they actually need to process that information. If not, they can simply opt to delete this as it's not necessary for their purpose.

Are you a UK broker who has a UK national living in the EU who insures their UK property with a UK based insurer?

A UK broker helps a UK national insure their UK property, but the client is living e.g. in Spain. If the individual is a UK citizen, then the UK GDPR will apply.

Helping you understand your situation

This short checklist can help you understand if you have an exposure to the changing rules.	✓	✗
Did you have customers, processors, contacts or employees in the EEA before the 1 January 2021?		
Do you have customers, processors, contacts or employees in the EEA at the moment?		
Will you continue to offer products and services to new customers or contacts in the EEA?		
Do any of your data processors process data outside of the UK?		
Do you have employees who are EEA citizens?		
If you have answered yes to any of the questions, you need to take action now.		

Guidance: actions you should take now

To help you understand what comes next and how to prepare, we have produced an outline of some of the key actions that firms can take now to manage ongoing compliance and awareness around the regulations and what additional measures might need to be put in place with or without a decision of adequacy.

Understand what activities might be impacted	Review and update your records of processing activities and consider what data might be affected.
Establish what "legacy" EEA Personal Data you processed prior to 31 December 2020	The EU GDPR as it stood on that date will apply to this data (frozen GDPR), so it's important that you can identify and easily separate that information. Although the UK and EU GDPR are the same, this could become more important should the UK GDPR change creating differences in which version of rules apply to which data.
Update your Privacy Notices and Data Protection policy frameworks	Any data being processed or stored outside of the UK is now a restricted/international transfer. You need to keep individuals informed and so must be transparent. You may also need to update any references to "Member State", "Union Law" or other EU GDPR terminology.
Data Protection Impact Assessments	You may need to update existing assessments in relation to UK GDPR. Check if they cover International Data Flows, which will become restricted transfers or refer to any EU GDPR terminology. Templates should be updated too.
Review your contacts and data processors and update your Record of Processing Activities and logs to identify which of those are in the EEA	You need to take stock and understand that even cloud and software solutions processing data in the EEA are now international transfers. You will also need to update privacy notices to ensure that you are being transparent about where data might be processed or stored, and, if ratified, adding transparency regarding the adequacy decision relating to EU-UK transfers.
Training and awareness	Review your awareness training and ensure that your key stakeholders and anyone responsible for processing personal data are aware of the potential changes and are kept in the loop with any plans or changes made.