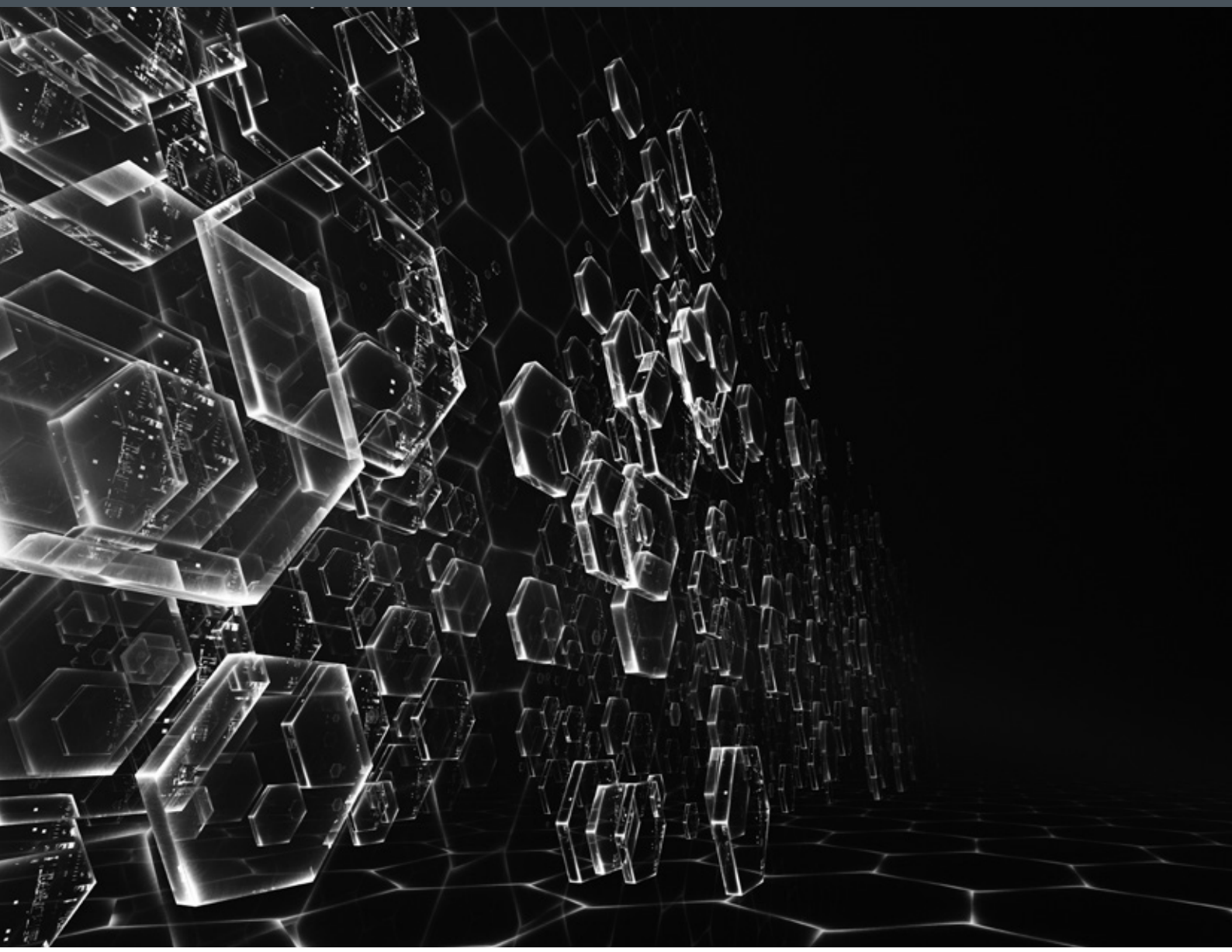


# GDPR TURNS THREE YEARS OLD
## OUR TOP TIPS MOVING FORWARD

The General Data Protection Regulation (GDPR) entered into force three years ago. Looking back we consider how the GDPR has shaped data protection regimes worldwide and shown its teeth by imposing large and often high profile fines. Looking forward, we set out our top tips to maintain compliance and report on the European Commission's adoption of new Standard Contractual Clauses (SCCs), respectively for use between controllers and processors in the EEA and for the transfer of personal data to third countries outside the EEA.

The GDPR came into force on 25 May 2018, establishing a new data protection regime in the EEA, which soon proved its global impact. Since then, we have seen companies adapt to the Regulation when collecting and/or processing personal data through conducting risk assessments by undertaking data audits and carefully drafting privacy notices and other policies, for example on data retention and data security. On the other hand, we have also seen large fines and a number of high profile data breaches. Looking ahead, the new SCCs for transfer of personal data to third countries outside the EEA include significant obligations for data importers, especially importers acting as controllers. For transfers of personal data to third countries from the EEA, the new SCCs (or an alternative safeguard), but not the existing SCCs, should be used for new transfer agreements after 27 September 2021; SCCs currently in effect must be replaced by the new SCCs by 27 December 2022. In this briefing we look back on the last three years, analyse the GDPR's impact and offer some top tips for companies moving forward.

## The GDPR at a glance

- Applies to both data 'controllers' and data 'processors', where the 'controller' decides how personal data will be processed and the 'processor' processes personal data on behalf of the 'controller'.
- Has extraterritorial effect and applies to transfers of personal data outside the EEA/UK.
- Applies to all companies and organisations that process personal data where:
  - the company or organisation is established in the EEA/UK;
  - the processing relates to offering goods or to services to data subjects in the EEA/UK; or
  - the processing relates to the monitoring of data subjects' behaviour within the EEA/UK.
- Imposes tight time limits for reporting data breaches to authorities and data subjects, if applicable.
- Gives data subjects rights, such as access to personal data and a right to be forgotten.
- 'Personal data' is widely defined as "any information relating to an identified or identifiable natural person" (or 'data subject'). This includes information such as names, passwords and biometric data.
- 'Data subject' is the natural person whose personal data is being processed.
- 'Processing' includes collection, storage, retrieval, alteration, dissemination and destruction of data.
- Processing of personal data is only lawful if one of six grounds apply, with three of the most commonly used grounds being consent; performance of a contract with the data subject; and the legitimate interests of the controller.
- Additional grounds apply to processing special category data (which includes information like ethnic origin, political opinions, religious beliefs, biometric data and health data).
- Following Brexit, the UK data protection regime closely mirrors the EU GDPR through the UK GDPR (being the retained EU GDPR) and the Data Protection Act 2018.

## GDPR in practice: Lawful grounds

Article 6 of the GDPR sets out the grounds under which data processing is lawful. Establishing a lawful ground is key to ensuring compliance with the GDPR and it is telling that a majority of the fines imposed have been for not establishing a sufficient legal basis for the relevant data processing. Although consent is a potential lawful ground, this can become problematic if records of consents received are not kept and updated. Furthermore, as consent can be withdrawn at any time, relying on it as a sole lawful ground can be tenuous. Over the last three years we have on the other hand seen 'legitimate interests' used widely in privacy notices as a lawful ground for data processing. Although initially envisaged to be used as a 'last resort', its wide definition has made it a useful tool for companies in maintaining compliance with the GDPR.

In practice, we can therefore expect the 'legitimate interests' ground to continue to be frequently used, but it is important to remember that the controller's or third party's legitimate interests must always be balanced against the rights and interests of the data subject. Therefore, it is recommended that a written legitimate interests assessment is conducted so as to demonstrate that this balancing test has been satisfied, consistent with the GDPR's principles of transparency and accountability.

## Heavy fines

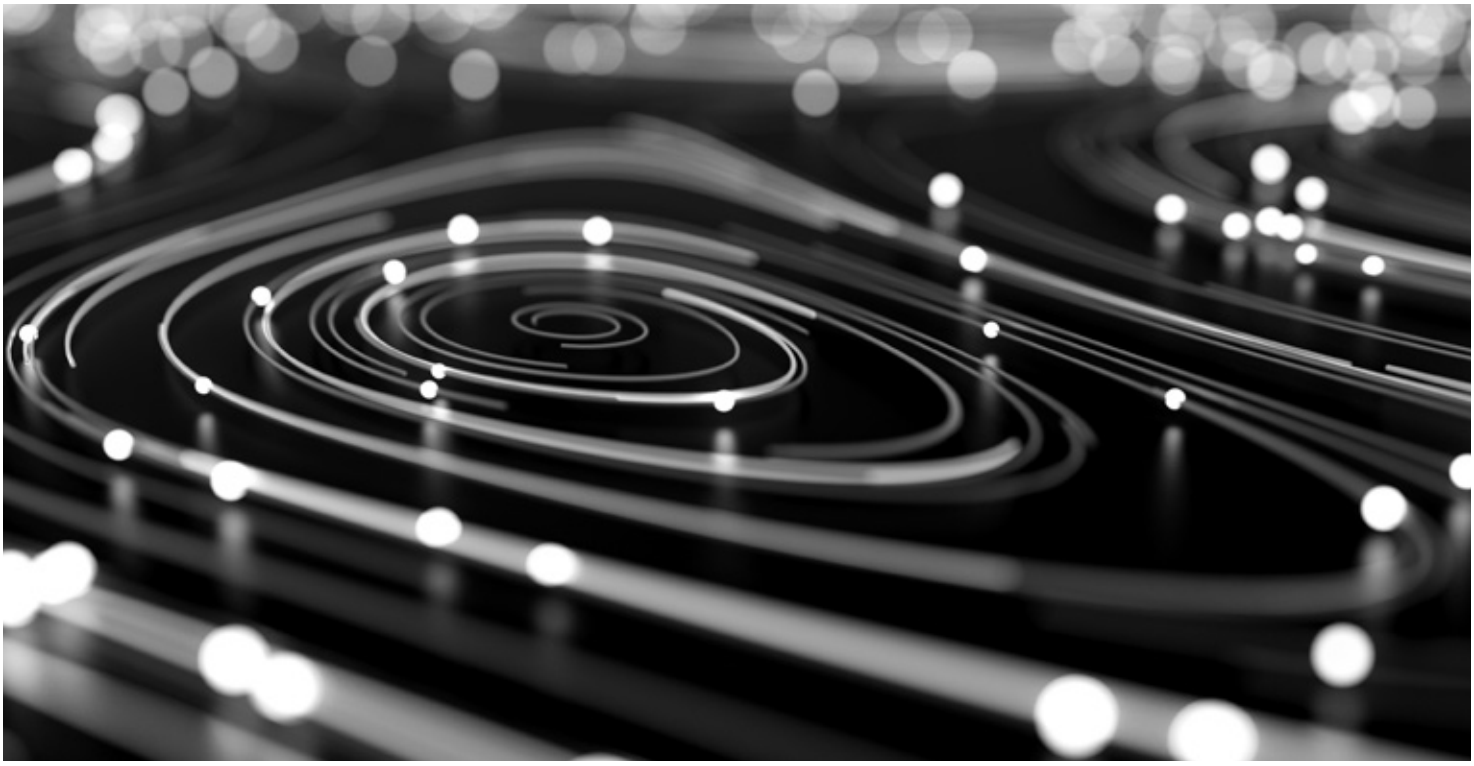
Infringements of certain GDPR provisions, for example the requirement that there is a lawful basis for processing personal data, can lead to fines of up to EUR20 million (£17.5 million in UK) or 4% of global annual turnover (whichever is higher). Fines over the GDPR's first three years total approximately EUR280 million, with the highest individual fine to date being the French authorities' EUR50 million fine against Google in January 2019. Other high profile fines include fines by the UK Information Commissioner's Office (ICO) against British Airways (GBP20 million) and Marriott International (GBP18.4 million). By imposing fines, regulators have shown that the GDPR has teeth.

Among the industry sectors with the largest amount and number of fines are Media/Telecoms, Transport & Energy and Insurance. It remains to be seen whether higher individual fines will be imposed (which will of course depend in part on the relevant company's annual turnover) and what industry sectors will be affected in the future.

## Global impact

The last few years have seen the passing of data protection and privacy laws worldwide. For example, in the UAE the financial free zones of the Dubai International Financial Centre and the Abu Dhabi Global Market have updated their data protection laws[1] and have reflected many of the

1 For more information, please see HFW's UAE Corporate and Commercial Bitesize Bulletin: https://www.hfw.com/UAE-CC-Bitesize-Bulletin-Issue-2-Sep-2020



principles of the GDPR and the state of California, USA has passed a new data protection law. Companies will increasingly need to consider what data protection regimes beyond the GDPR apply to the personal data they collect and process.

Linked to the GDPR's global impact are also the European Commission's adequacy decisions that determine whether a non-EEA country has an adequate level of data protection to allow data transfers to it from the EEA without a safeguard.[2] The European Commission is yet to publish its adequacy decision on the UK, with EU-UK transfers of personal data continuing unrestricted until at least 1 July 2021 (transfers of personal data from the UK to the EEA are unrestricted at least for a transition).

### Standard Contractual Clauses

On 4 June 2021 the European Commission adopted and published two sets of new SCCs, one for use between controllers and processors in the EEA and the other for the transfer of personal data to third countries outside the EEA.[3] They reflect new requirements under the GDPR and take into account recent case law. The SCCs for transfers to third countries can be used for the following transfers: controller-to-controller; controller-to-processor; processor-to-controller; and processor-to-processor.

The Decisions adopting the new SCCs will enter into force on 27 June 2021. Previous Decisions adopting SCCs for international transfers will be repealed on 27 September 2021. Contracts incorporating SCCs for international transfers made under the previous EU data protection legislation will remain valid until 27 December 2022, provided processing operations remain unchanged and are subject to appropriate safeguards.

Given the limited transition periods, businesses should act quickly to analyse their current compliance with the new SCCs, their data transfers and their related contractual obligations. They may need to update compliance policies and templates and conclude new SCCs for current and future transfers.

The new SCCs for transfers of personal data outside the EEA include obligations on controller importers to give notices to data subjects and to notify personal data breaches to EU authorities. The parties must warrant that they have no reason to believe that the laws and processes in the importing country prevent the importer from fulfilling its obligations under the new SCCs. They, and parties to existing SCCs, should conduct and document risk-based assessments of the laws in the importing countries. These assessments should be revised following any changes to the relevant legal framework and made available for review by supervisory authorities on request.

There are situations where additional supplementary measures will need to be implemented to ensure that data subjects are given a level of protection which is equivalent to that within the EU.

The UK Information Commissioner's Office is preparing bespoke SCCs under the UK GDPR and plans to consult on them shortly.

### Conclusion

Three years on, we see that the GDPR is still in its infancy with all relevant parties, be they processors, data subjects or regulators, still finding their feet. Many countries outside the EEA have developed or are developing their own data protection regimes and data subjects are becoming more aware of their data processing rights. Companies should therefore remain alert and follow our top tips to avoid the risk of facing hefty fines and/or reputational damage.

2 For a full list of countries that the European Commission has to date determined provide adequate data protection, see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

3 The European Commission's new SCCs are available at ec.europa.eu/commission/presscorner/detail/en/ip_21_2847

# TOP TIPS

After three years of living with the GDPR, we set out our top tips for companies to achieve compliance and avoid violations:

- If you detect a data breach, assess promptly whether it should be reported to regulators and data subjects
- Ensure that all staff are trained and also update staff regularly through refresher trainings
- Keep reviewing processes and run regular checks – be prepared for an investigation by the regulator
- Keep records of data processing and ensure you know what categories of data are processed and the reasons for holding the data
- Check email addresses and attachments before sending – do not underestimate the human factor in data breach risks
- Keep up to date with the latest guidance from your regulator – policies should be under constant review
- Consider the extent and limitations of the legitimate interests ground – it is the most flexible basis for collecting and processing personal data but the balancing test as against the data subject's interests must be satisfied
- Do not rely too heavily on the consent ground as the lawful basis for collecting and processing data – consent can be withdrawn at any time!
- Update SCCs used for the transfer of personal data from the EEA (and in due course the UK) to third countries outside the EEA
- Consider using new SCCs for transfer of personal data between controllers and processors in the EEA

For further information please contact the authors of this briefing;


**ANTHONY WOOLICH**
Partner, London
**D** +44 (0)20 7264 8033
**E** anthony.woolich@hfw.com

**JEMIMA MCDONALD**
Senior Associate, Abu Dhabi
**D** +971 2 235 4911
**E** jemima.mcdonald@hfw.com


Assistance provided by Johanna Ohlman, Trainee Solicitor.