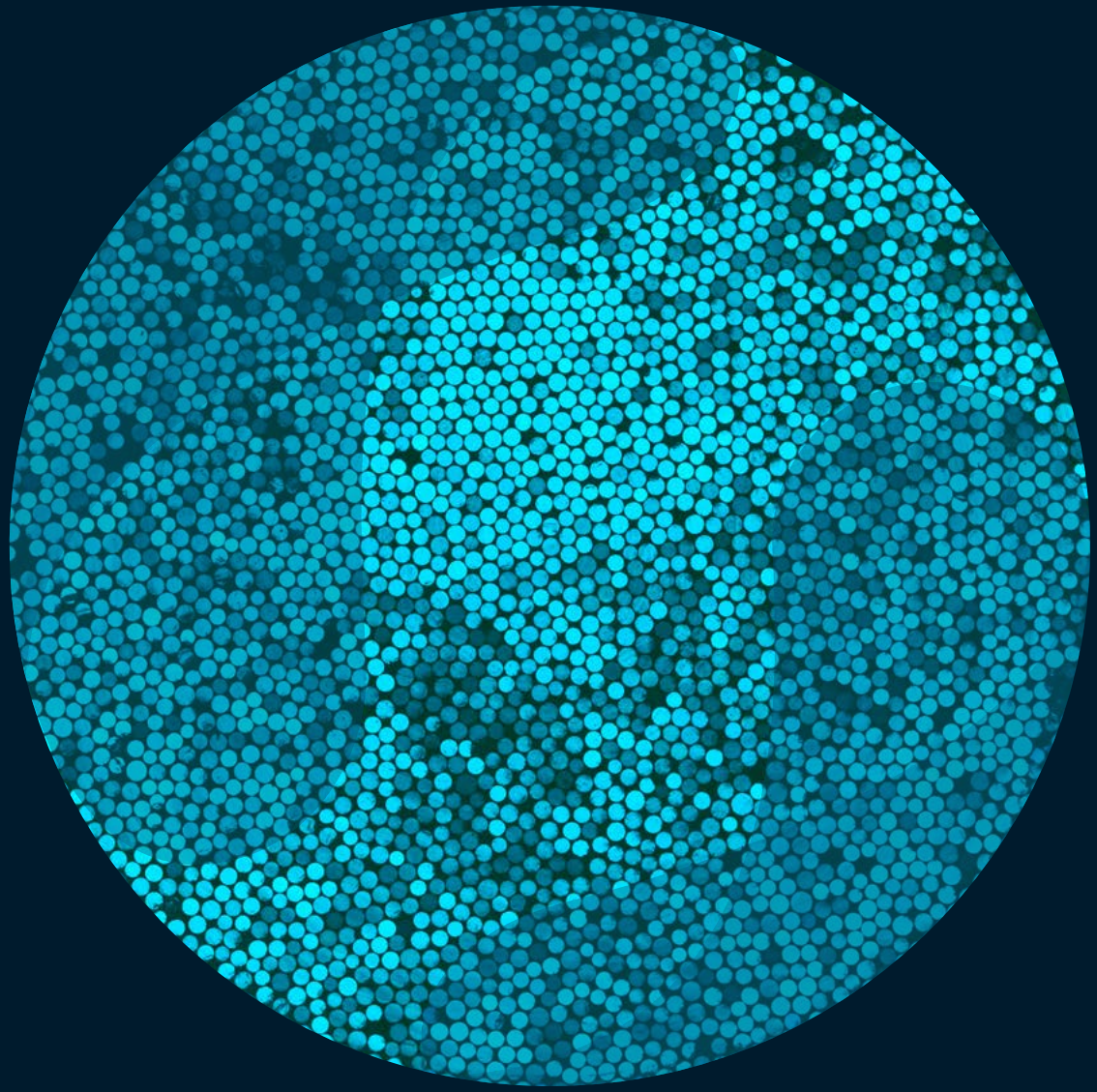


Unsettled Status

AN UPDATE ON INTERNATIONAL
DATA TRANSFER LAW

For what comes next
tlt.com

TLT | holla | GSJ advocaten

Contents

Back to contents

Introduction

The international data transfer landscape has undergone wholesale changes in recent years, and remains incredibly unsettled. The introduction of the General Data Protection Regulation (GDPR) in 2018, alongside both the UK's departure from the European Union (EU) and the landmark judgment in the Schrems II case in 2020, have altered data transfer law significantly, ultimately creating uncertainty and risk for organisations in the UK, the EU and worldwide.

And while the impact of these developments has not yet been fully realised, there could be far-reaching consequences that many organisations may not be fully prepared for.

With deadlines to meet new requirements approaching, this paper outlines the scope of the changes to international data transfer law, the challenges they present, and how organisations across all sectors can prepare for them.

“The international data transfer landscape has undergone wholesale changes in recent years, and remains incredibly unsettled.

Back to contents

The changes and challenges

GDPR and Brexit

Two major events that have impacted data protection laws in recent years are the introduction of the GDPR and Brexit.

Introduced in May 2018, the GDPR was intended to harmonise data protection laws across the EU. This, in turn, was expected to remove barriers and streamline the regulatory regimes that EU and international organisations needed to adhere to, while reducing the cost of compliance. However, gaps or optional positions within the fine print of the GDPR meant that member states could in some circumstances draw their own lines in the sand. These inconsistencies and local variances have added to the compliance burden, despite the core GDPR text being consistent across the EU.

The UK's subsequent departure from the EU caused more uncertainty, bringing the need for new, rapid changes to data protection laws. This was primarily due to the UK now being considered a 'third' country by the EU for data protection purposes. This meant that data controllers in the EU would need to identify an appropriate safeguard to enable the transfer of data to the UK – a step that was not previously necessary. An exit from the EU was an exit from its data protection circle of trust.

An unstable agreement

Both the UK and EU recognised that there would be a significant cost in preventing data transfers from continuing between them. One study concluded that the cost to UK organisations alone would be between £1bn and £1.6bn[1]. Consequently, it was agreed to implement a formal adequacy decision.

> Both the UK and EU recognised that there would be a significant cost in preventing data transfers from continuing between them.

In data protection, 'adequacy' is used by the EU to define other 'third' countries, as well as territories, specified sectors, and international organisations, which can offer an 'essentially equivalent' level of data protection and thus legal certainty and uniformity to its member states. An 'adequacy decision', therefore, is the process by which a third country is recognised as adequate.

On 28 June 2021, the European Commission (EC) adopted two adequacy decisions for the UK to facilitate transfers of personal data from the European Economic Area (EEA) to the UK under the GDPR and Law Enforcement Directive, which regulates access to personal data by law enforcement bodies. The UK also reaffirmed its previous position of deeming all countries within the EEA as adequate. In essence, this dual agreement meant that data could continue to flow freely between the EU and the UK (and vice versa) without the need for any additional safeguards to be implemented.

However, this agreement is fragile and temporary, which could present significant challenges to organisations in the UK and the EU. Unlike other decisions of their kind, the current adequacy decisions include a 'sunset clause', which strictly limits their duration. Instead of remaining indefinitely, they are set to automatically expire after four years. After this time, the adequacy findings *might* be renewed – but only if the UK continues to ensure a level of data protection that is deemed adequate by the EU. This is far from a given, as the UK appears intent on writing its own data protection laws.

> However, this [adequacy] agreement is fragile and temporary, which could present significant challenges to organisations in the UK and the EU.

Adding to this uncertainty is the fact that the EC is keeping the UK's adequacy status under close review during this four-year period. Should the UK diverge too far from the EU's approach, an intervention could see the EU's original adequacy decisions revoked. While this is fairly unlikely, it casts an unwelcome shadow over the agreement. But if the UK changes its laws to divert away from the GDPR or grant its own adequacy decisions in favour of third countries with which the EU does not agree, then the EC could intervene at any point.

1 https://neweconomics.org/2020/11/uk-companies-could-face-new-costs-up-to-1-6bn-if-the-eu-doesnt-deem-the-uks-post-brexit-data-protection-standards-adequate

The case of Schrems II

There is an additional factor surrounding international data transfers that has brought its own challenges: the judgment in the Schrems II case, which was handed down by the Court of Justice of the European Union (CJEU) on 16 July 2020.

The case itself originated from data privacy activist Maximilian Schrems calling for the Irish Data Protection Commissioner to invalidate the EC's Standard Contractual Clauses (SCCs) for Facebook's use of personal data transfer to its US headquarters. As pre-approved language that can be inserted into contracts to enable legal data transfers between the EU and third countries, SCCs are by far the most commonly used safeguard and mechanism for data transfers. Global companies like Microsoft and Amazon use SCCs, and according to a 2020 data transfer survey, they are used by 85% of companies in Europe[2].

In the 2020 case, Schrems argued that the data in question could be accessed by US intelligence agencies, which would be in violation of the GDPR and EU law.

The CJEU declared that the EU-US Privacy Shield, which was previously used to legitimise data transfers from the EU to the USA, was invalid, meaning that with immediate effect it could no longer be relied upon to export data to the US. According to the CJEU, US surveillance programmes were not limited to what was strictly necessary and proportionate. It also pointed out that EU-based data subjects lacked actionable judicial redress and the right to an effective remedy in the US. It further shone a light on some issues with SCCs, on how they are used in practice and on the need for case-by-case assessments of the sufficiency of foreign protections, prompting the EC to set about drafting new versions; a task that many data protection lawyers believed was long overdue.

Despite the judgment being handed down more than two years ago, the impact of Schrems II is still evolving. These new SCCs were introduced by the EU on 27 June 2021, with organisations granted a three-month transition period in which they could continue to conclude contracts based on the old SCCs. After this period though, both EU-based data exporters *and* organisations based outside of the EU that process personal data of EU data subjects were required to use the new version of the SCCs for any new contracts.

An 18-month grace period was included in this transition, during which data exporters must amend any existing contracts to replace the old SCCs. This grace period ends on 27 December 2022. However, organisations need to replace the old SCCs before that date if the data processing operations governed by the contract are modified during said grace period. After 27 December 2022, any contracts that still contain the old SCCs will be non-compliant with the GDPR and vulnerable to challenge. With this deadline just months away, there is an urgent need for organisations that transfer data outside the EU to act now and ensure they are in line with these new SCCs.

> With this deadline just months away, there is an urgent need for organisations that transfer data outside the EU to act now and ensure they are in line with these new SCCs.

Key deadlines

- **27 December 2022**
  Grace period ends for replacing old EU SCCs
- **21 March 2024**
  Grace period ends for replacing old UK SCCs

2 https://www.digitaleurope.org/news/schrems-2-data-transfers-survey-85-of-companies-in-europe-use-standard-contractual-clauses/

Navigating the changing landscape

The combination of the GDPR, Brexit and Schrems II has changed the face of international data transfers dramatically. And the consequences of these changes will have implications for more organisations than just those directly involved in data transfers.

If an organisation uses common IT platforms like Microsoft Teams or Salesforce, it may be faced with the challenges brought on by new data transfer laws. With this in mind, it's important that organisations understand their level of exposure and how they can manage the impact of these changes.

UK and EU: diverging paths

While Brexit is promoted by the UK government as part of a more pragmatic, 'pro-business' approach, this means that there may be further divergence from the EU position in the future. The UK government has publicly indicated that it is likely to adopt a different approach to its assessment of third countries, and its **list of priority countries** includes nations that have not been deemed adequate by the EU.

> The direction of travel has been made even more clear by the UK's adoption of its own SCCs.

The direction of travel has been made even more clear by the UK's adoption of its own SCCs. Referred to as the International Data Transfer Agreement (IDTA), it was drafted by the UK's data protection authority, the Information Commissioner's Office (ICO). On 21 March 2022, the UK parliament approved the IDTA and an addendum to the EC's new SCCs, with a grace period for updating contracts that currently use the old SCCs ending 21 March 2024.

Organisations that operate across the EU and the UK are likely to be directly impacted by these changes. For example: if an organisation is headquartered in Brussels but has a presence in the Netherlands and the UK, and exports data from all three jurisdictions to the US, then it would need to repaper its existing contracts that include the old SCCs to reflect the new SCCs for EU to third country data transfers, as well as the IDTA for UK to third country data transfers.

Alas, there are an increasing number of hoops for organisations to jump through, and with less than 18 months until the last grace period ends, the clock is ticking. More often in this type of scenario, organisations are keen to change their contracts only once, for all EU and UK jurisdictions, to ensure that the contract terms remain consistent. They are therefore pushing hard to complete all of the repapering (for both the EU and the UK) by the EU's 27 December 2022 deadline. This is in most cases a challenging timescale, given the volume of contracts impacted by the changes.

> More often in this type of scenario, organisations are keen to change their contracts only once, for all EU and UK jurisdictions, to ensure that the contract terms remain consistent.

The UK's addendum to the EC's SCCs does offer a potential solution. Alongside the full version of the IDTA, the UK addendum can be used as an alternative to validate data transfers from the UK to a third country – it acts as a "bolt on" to the EC SCCs. This will be particularly useful for multinational organisations sending data from both the EU and the UK to a third country, as it will allow the organisation to maintain a consistent set of terms across each jurisdiction, rather than having a separate IDTA for the UK.

With the new SCCs and IDTA in place, the future contractual model looks more certain. But there is one final stumbling block that organisations must bear in mind. Now, they must undertake a transfer risk assessment, or data transfer impact assessment (DTIA), before exporting any data to a third country that has not already been declared adequate. This point was reiterated in the Schrems II judgment given the need for case-by-case assessments of the sufficiency of foreign protections, and is something to which data protection authorities across the EU and UK are now paying close attention.

Undertaking a Data Transfer Impact Assessment

In the Schrems II case, the CJEU took the opportunity to remind organisations and EU institutions that it is not enough to simply insert an SCC into a contract and conclude that the data transfer to a third country is appropriate. Instead, the data exporter should actively consider the laws and practices of the destination country, along with any additional measures that may need to be implemented to ensure that the transfer is compliant with data protection legislation.

In order to assess which additional measures are appropriate on a case-by-case basis, the data exporter in the EU may conduct a DTIA. A step-by-step guide recommended by the European Data Protection Board (EDPB) can be found **here**, but some practical steps that can assist organisations when conducting a DTIA are:

a. **Map data flows:** Understand exactly what internal and external international data transfers are being undertaken by your organisation, which tools are being used, and what additional safeguards are required or preferred for each transfer.

   When mapping the data flows of your organisation, you should also take into account further transfers, for example from a processor in a third country to a sub-processor in a different third country.

b. **Contract remediation:** Identify and risk assess which of your existing contracts (i) rely on the old SCCs and therefore need to be replaced with the new EU SCCs, (ii) may also need the proposed new UK addendum bolt on, and (iii) may only require the UK IDTA.

c. **Transfer risk assessment:** Embed a process of undertaking transfer risk assessments for relevant transfers, understanding how to identify where a transfer risk assessment is required and how to identify and implement any relevant additional measures.

   The DTIA requires an assessment of whether the legislation or practice of the third country could undermine the effectiveness of the transfer instrument used by your organisation. In this assessment, your organisation should pay particular attention to the relevant legislation of the third country that might undermine the level of protection. An example of this would be legislation that allows public authorities to access personal data for oversight purposes, or lack of the right to an effective remedy.

   Following this assessment, your organisation should determine whether any additional measures are needed to achieve a level of protection similar to that in the EU.

d. **Update template contracts:** Ensure the inclusion of the new SCCs and a watching brief for UK IDTA across any existing template contracts still in use.

e. **Lead supervisory authority:** Identify and begin to engage with a lead supervisory authority in the EU.

f. **Policy review:** Review and update policies and privacy notices to reflect Brexit and other key events that impact legislation.

g. **Assess protection regularly:** Re-evaluate protection levels at appropriate intervals and monitor developments that may have an impact on the level of protection.

In addition, UK companies that fall within the territorial scope of the GDPR but have no establishment in the EU should consider whether to designate an EU representative.

Binding Corporate Rules: an alternative?

The additional effort now required of organisations to undertake transfer risk assessments, alongside the vulnerability of the new SCCs to further challenges from privacy activists, has seen more and more organisations consider implementing Binding Corporate Rules (BCRs). BCRs are implemented to govern intra-group data transfers across multiple jurisdictions but have not been popular historically. They take a long time to implement, can be expensive and previously were more complex than the simpler route to compliance that SCCs offered.

Now though, the popularity of BCRs is surging. For those organisations that have enhanced their privacy functions since the introduction of the GDPR in May 2018, much of the groundwork for a successful BCR application might have already been completed.

> Now though, the popularity of BCRs is surging.

Whether a BCR is right for an organisation can depend on a number of factors. Brexit has meant that companies operating in both the UK and the EU will have to submit separate applications for the two legal regimes. Trickier still, a competent supervisory authority must be decided upon, which can be time consuming but even more importantly, represents a particular challenge for UK-based organisations that are looking to identify and establish an EU-competent authority, since previously they would have relied on the ICO in the UK to perform this function.

Finally, UK organisations that process personal data relating to EU-based data subjects must appoint a lead EU supervisory authority (which differs from a competent supervisory authority). If the organisation had previously identified the ICO as its lead authority, and has no genuine main establishment in the EU, then the process will likely prove difficult. The reward though, is benefiting from the wide protection of a BCR.

More changes, more uncertainty

With deadlines looming, organisations should examine their data transfer policies now and prepare carefully for the upcoming changes. They should also prepare to expect more changes to international data transfer laws in the future, as the impact of Brexit and the Schrems II case continue to influence data protection in the UK, the EU and around the world.

In particular, there should be a focus on the approach taken by the UK government towards adequacy decision making, and on any reforms that it introduces to the UK GDPR and Data Protection Act. The introduction of the Data Protection and Digital Information Bill on 18 July 2022 may also bring further changes to UK policy once it becomes law, and this could trigger yet further points of difference from EU data law.

Already we're seeing divergent approaches emerge between EU and UK data protection authorities when it comes to enforcing rules on international data transfers. Some regulators are taking a very firm line, and this is contributing to a 'data localisation' agenda in some areas, whereby organisations taking on work must guarantee information remains within its operating location. But this contrasts with the GDPR's recognition that "flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation"[3].

> Already we're seeing divergent approaches emerge between EU and UK data protection authorities when it comes to enforcing rules on international data transfers.

Whether European regulators and legislators work to harmonise these apparently conflicting perspectives in the coming months and years remains to be seen. However, it is clear that recent events are already having a broad and tangible impact upon the decisions made by both EU and UK authorities.

Further, there is confusion surrounding the GDPR and the EU's new SCCs. This is evident in a recent decision made by the Belgian Data Protection Authority regarding the Transparency & Consent Framework. This framework was designed by industry trade group IAB Europe as a direct response to the GDPR and was widely used in the digital advertising industry, including real time bidding. However, IAB Group, which did not consider itself a 'data controller', was ultimately found to have infringed the GDPR through unauthorised data processing, because the Belgian Data Authority ruled that it *was* in fact a data controller, referring to the broad interpretation of "controller" given by the EDPB and the CJEU [4]. Other organisations could find themselves caught out in similar ways.

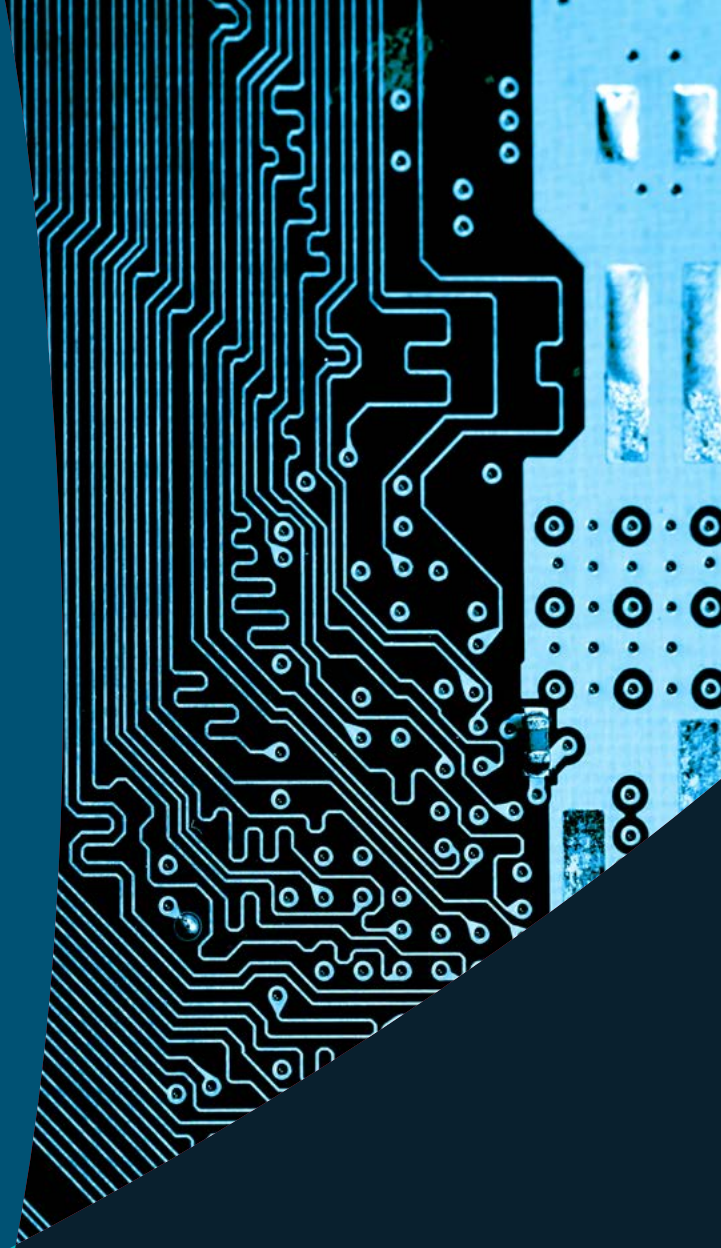
3 Recital 101, EU GDPR

4 EDPB – Guidelines 7/2020 on the concepts of controller and processor in the AVG, v2.0, para. 20; CJEU, 10 July 2018, C-25/17, ECLI:EU:C:2018:551

How we can help

Acting now to address the changes to international data transfer law will give organisations the best chance of minimising future disruption to their operations. The vulnerability of an organisation to the pending changes will depend on the location and sector in which it operates, but TLT, Holla legal & tax and GSJ Advocaten can support you to navigate the changing landscape with confidence. Get in touch with our expert data, privacy and cybersecurity teams today.

TLT, Holla legal & tax and GSJ Advocaten are strategic alliance partners, who joined forces to deliver international cross-border services for our clients. From an established network of offices in the UK, the Netherlands, Belgium and beyond, we actively share knowledge, expertise and innovation to provide organisations with seamless cross-border advisory, disputes and transactional services.



TLT | holla | GSJ advocaten

About TLT

For what comes next

We're your business advisers as well as your lawyers, working in step with you to protect your interests today and progress your ambitions for tomorrow.

With local, national and international reach, we draw on our diverse expertise to find solutions and look ahead to create new opportunities.

We support large corporates, public institutions and high growth businesses on their strategic and day-to-day legal needs. Our offering includes market-leading legal expertise, near-legal consultancy services and a suite of solutions developed under our FutureLaw innovation programme.

With significant experience advising organisations in the digital; financial services; future energy; leisure, food & drink; government and public services; real estate; and retail & consumer goods sectors, we have a strong track record of consistent growth driven by client need.

TLT has over 140 partners and employs around 1,300 people.

tlt.com

Gareth Oldale
Partner | Data, Privacy & Cybersecurity

T +44 (0)333 006 1595
E gareth.oldale@tltsolicitors.com

Gareth is a partner and head of **data privacy and cybersecurity** at UK law firm TLT.

He provides commercially strategic advice to a range of clients across the private and public sectors, with a core focus on technology projects. He specialises in data protection, privacy and information law matters, having advised in this area throughout his career.

Gareth advises on the full range of data protection matters, including: compliance audits; privacy by design; data ethics; artificial intelligence and biometrics; data organisational design; data and cyber breaches; and international data transfers. He also acts as external data protection officer for a number of clients.

Gareth is often invited to speak at external conferences and seminars on data protection matters, and is a regular contributor to specialist journals including the Privacy & Data Protection Journal and Privacy Laws & Business. In addition, he is frequently asked to provide comments for the national press on high profile data breaches, including the Financial Times, BBC, The Times, ITV News, The i Newspaper, Business Leader and Huffington Post.

Louisa Williams
Legal Director | Data, Privacy & Cybersecurity

T +44 (0)333 006 1359
E louisa.williams@tltsolicitors.com

Louisa is a data protection specialist, experienced in helping clients to navigate the evolving landscape of data protection regulation across the UK and the EU.

She advises on a wide range of strategic issues, including taking the lead on largescale GDPR compliance programmes, advising on complex data sharing arrangements and international data transfers, undertaking data protection impact assessments, handling largescale personal data breaches, and assisting clients in engaging with data protection authorities on a variety of topics.

Louisa has experience in numerous sectors including the **public sector**, **financial services** and **digital sector**. She has also undertaken a number of client secondments, including at the Financial Conduct Authority. She is able to use this first-hand, practical experience to provide strategic and commercial advice to her clients.

About Holla

Local Hearts, Global Minds

We are Holla Legal & Tax, a leading corporate law firm in the Netherlands. Our specialist lawyers operate in close-knit teams, aligning with your interests in order to keep you ahead of the curve. We help you tackle your legal challenges and preferably even prevent them from arising. We support a wide array of clients in the corporate and public domain, including listed corporations, enterprises, government bodies, non-profit organisations and care institutions.

With local offices in Utrecht, Den Bosch and Eindhoven, we have a strong track record in the Netherlands. Our specialists know and understand your sector and local market. But your professional and legal interests are not limited by country borders. International developments are having a direct impact on your organisation. Our cross-border expertise and the seamless legal support by our premier alliance partners has become increasingly relevant. We call this Local Hearts, Global Minds.

holla.nl

Kim de Bonth
Partner | IP, ICT & Privacy

T +31 88 4402 347
E k.debonth@holla.nl

Kim heads Holla's Data Protection & Privacy team. Kim is highly specialised in data protection legislation and is a Certified Information Privacy Professional (CIPP/E).

As Kim has been assisting some of her clients for over two decades, she has gathered great knowledge of their industries, including healthcare and welfare, business services, e-sports, energy and innovation. As such, Kim brings a depth of strategic legal expertise. She works extensively with general and staff counsel providing coordination and support for complex affairs.

Kim counsels clients on all matters related to privacy, data and security. Kim is also regularly invited to speak at conferences about her area of expertise.

Femmie Schets
Associate | IP, ICT & Privacy

T +31 88 44 02 333
E f.schets@holla.nl

Femmie advises and litigates in matters involving privacy, intellectual property, and ICT, including commercial contracting. Recently, Femmie also became a Certified Information Privacy Professional (CIPP/E).

Within her expertise, Femmie focuses on privacy and data protection law in various sectors, including the healthcare and welfare sector, business services, telecom, auditing and the (international) gaming industry. She deals with a wide range of matters, from drafting privacy statements to advising on international data transfers and data breaches. Femmie regularly publishes news items on these topics.

About GSJ

About GSJ

GSJ is a full-service law firm located in Antwerp, Belgium. Our team of 18 partners and 65 lawyers specialise in sectors such as banking and insurance, real estate, retail, industry, public sector, education and health care.

As one of Antwerp's largest law firms, GSJ has been the legal partner for public authorities, businesses and private individuals in various sectors and for international clients operating in Belgium.

Our firm is divided into 6 departments that overlap and drive each other. The result is cross-pollination that expands and strengthens the knowledge of the lawyers. Through this exchange, every client at our law firm has access to professional knowledge in a variety of fields.

Our motto "a problem shared is a problem halved" has resulted in an open structure, in which exchange of knowledge and cooperation are key.

gsj.be

Geert Philipsen
Partner | Commercial, Retail & Regulatory, Competition & EU Law

T +32 3 201 14 29
E geert.philipsen@gsj.be

Geert Philipsen joined GSJ in 2000, where he subsequently became a partner in 2008.

Geert has focused mainly on offering his services as an expert on intellectual property law, in which capacity he uses his training to provide timely advice, to draw up and negotiate contracts relating to the many aspects of intellectual property and to assist clients with procedures in these fields. Within the context of intellectual property law, Geert has also acquired a wealth of experience in the area of data protection, privacy and market practices.

In the fields of intellectual property law and market practices, on several occasions Geert has handled cases before the Benelux Court of Justice and the CJEU. He has also worked extensively in the area of distribution and, more generally, national and international commercial contracts.

Kristien Wevers
Senior Associate | IP, ICT & Privacy

T +32 3 201 14 29
E kristien.wevers@gsj.be

Kristien launched her career with GSJ in 2012. She mainly focuses on cases concerning ICT law, protection of personal data (GDPR), privacy, ecommerce, intellectual property rights, protection of trade secrets (know-how), media law and market practices.

In the field of intellectual property, she advises clients and assists them with the protection of creations, distinctive signs and inventions.

With regard to data protection and privacy, Kristien supports companies with all of their compliance activities.

Furthermore, Kristien focuses on the negotiation and drafting of contracts and legal documents on all matters related to data protection (e.g. data processing agreements), ICT and intellectual property.

In addition, Kristien assists clients in proceedings relating to these matters. In the field of intellectual property law, she has already conducted proceedings before the Benelux Court of Justice.

Kristien has also been invited to speak at seminars and to publish articles on data protection matters.

Recently, Kristien became member of the International Association of Privacy Professionals (IAPP)

tlt.com/contact

Belfast | Bristol | Edinburgh | Glasgow | London | Manchester | Piraeus | Utrecht | s-Hertogenbosch | Eindhoven | Antwerp