

The Data Privacy Chronicle

Edition # 3 - Intragroup data transfers: A blind spot for international groups

Do you really have your intragroup data transfers under control?

The Data Privacy Chronicle is a sequence of pragmatic newsletters mainly designed for Data Protection Officer (“DPOs”), privacy leaders and their respective organisations. The aim is simple: to provide you with practical insights, powered by our experience as data protection lawyers and DPO-as-a-Service providers, on emerging topics that shape your role and to help you navigate the growing complexity of regulatory frameworks in the digital era.

This new edition focuses on a topic that is often underestimated in practice but increasingly investigated by supervisory authorities: **intragroup international data transfers**.

1. Why intragroup data transfers deserve attention today

Intragroup data transfers have long been perceived as a secondary issue in data protection compliance. In many international groups, the focus remains on external data sharing, vendors, and outsourcing arrangements, while internal data flows are assumed to be inherently safer due to common ownership, aligned interests, and internal policies. This assumption, however, is increasingly in conflict with the General Data Protection Regulation (hereinafter “GDPR”) framework and supervisory practices.

Under the GDPR, the concept of “transfer” is not linked to the existence of a contractual or corporate relationship, but to the practical circumstances under which personal data is made accessible to another entity. From a regulatory perspective, the fact that two entities belong to the same group does not neutralise the risks associated with international data transfers. Indeed, complex group structures often multiply such risks by creating diffuse, unclearly documented and constantly evolving data flows.

As a result, intragroup data transfer agreements (hereinafter “IGDTAs”) have become a fundamental, often overlooked, compliance tool. Their absence often constitutes a hidden risk, especially in groups with a strong international presence and decentralized operations.

One of the most persistent misconceptions among international groups is the assumption that internal data flows are, by definition, low risk. This perception is often rooted in the belief that group entities share a common compliance culture, that internal access to personal data is inherently easier to monitor and control, and that existing intragroup policies or data processing agreements already provide sufficient safeguards. While understandable from an operational perspective, these assumptions do not align with

the regulatory approach under the GDPR, which focuses on accessibility and jurisdiction rather than corporate affiliation.

In practice, intragroup data flows often involve continuous or structural access to EU personal data through centralised systems, shared platforms or global support functions. Where such access is exercised from jurisdictions that are not formally recognised by the EU as providing an adequate level of data protection, organisations must implement appropriate safeguards to legitimise the transfer. In the absence of a clear contractual and governance framework, demonstrating compliance may become particularly challenging.

These scenarios often remain under the radar because they do not resemble traditional data exports. Remote access to EU systems by non-EEA teams, the use of global HR or finance tools administered from abroad, or cross-border access by audit, risk or IT functions may appear as routine internal arrangements, however, even where no data is physically transferred, such access can still trigger the international transfer rules set out in the GDPR.

Why this is particularly relevant for Luxembourg-based groups?

Luxembourg occupies a unique position within the structures of international groups. Many entities based in this country, even those with limited staff, have considerable access to personal data relating to employees, investors, or counterparties located in multiple jurisdictions. By contrast, Luxembourg-based entities often grant access to such data to group entities located outside the EU, particularly in the context of global support functions.

This dual role significantly increases exposure to issues related to international data transfers. At the same time, Luxembourg's supervisory authority (*Commission nationale de protection de données* or *CNPD*) has shown a growing interest in the content of data flows, rather than their formal classification. During audits, inspections, or due diligence exercises, intragroup transfers are increasingly being examined as a separate compliance issue, especially when no specific contractual framework exists.

In this context, it is no longer sustainable to consider intragroup data transfers as a secondary issue. For Luxembourg-based groups, the absence of a properly structured IGDTA can quickly turn from a weakness into a concrete risk.

2. What is an intragroup data transfer agreement?

The regulatory framework governing intragroup data transfers is primarily set out in Chapter V of the GDPR, which establishes the conditions under which personal data may be transferred to recipients located outside the European Economic Area. While the wording of the GDPR does not single out intragroup scenarios, supervisory authorities and EU courts have consistently clarified that intragroup transfers are not subject to a lighter regime merely because they occur within the same corporate group.

A **key starting point** is the definition of what constitutes an international data transfer. Although the GDPR does not explicitly define the term, guidance from the European Data Protection Board (EDPB) has clarified that a transfer occurs where a controller or processor subject to the GDPR discloses or makes personal data accessible, to another controller or processor located in a third country or international organisation.

As confirmed by EDPB Guidelines 05/2021, this includes situations involving remote access, support activities or centralised processing, even in the absence of any physical movement of data. From an intragroup perspective, this clarification is particularly relevant: access by a non-EEA group entity to systems hosted in the EU, or the use of global tools administered from outside the EEA, may trigger Chapter V obligations regardless of where the data is technically stored.

Data Protection authorities focus: beyond the US and China

In this context, supervisory scrutiny is not limited to a small number of well-known jurisdictions. While transfers to the United States or China often attract attention, the underlying regulatory expectation applies to any third country.

More generally, the practice of the CNPD and its equivalents in other countries confirms that any transfer to a third country without an adequacy decision, that is, without a formal recognition by the European Commission that the third country ensures an equivalent level of data protection as the one provided under the GDPR, must be assessed on the basis of that country's national legal framework. For international groups, focusing compliance efforts on a limited number of jurisdictions may therefore create blind spots, as intragroup access to personal data from regions with different regulatory frameworks can raise issues that only become apparent during audits, inspections, or transactional due diligence.

3. What is an Intragroup Data transfer agreement? (and what is it not)

An IGDTA is a contractual framework governing the conditions under which personal data is transferred between entities belonging to the same corporate group, where such transfers qualify as international data transfers. Its purpose is not merely formal, but operational: to ensure that transfer safeguards are implemented consistently and effectively across the group.

When is an IGDTA required?

The need for a dedicated intragroup framework depends on several factors, including:

- the qualification of the parties (controller-to-controller vs controller-to-processor),
- the direction of the transfer (EU to non-EU),
- and the nature of the access (storage, remote access or support).

In practice, groups often operate hybrid models combining several of these scenarios, making fragmented or ad hoc contractual solutions ineffective.

Common misconceptions and ineffective solutions

Experience shows that intragroup transfer risks are frequently underestimated due to recurring misconceptions, such as:

- “We already have DPAs in place, so we are covered”,
- over-reliance on standard contractual clauses without operational alignment,
- the use of global templates disconnected from actual data flows.

While these tools may form part of the solution, they rarely provide sufficient coverage on their own.

4. Identifying intragroup data transfers: easier said than done

Before assessing safeguards or drafting intragroup data transfer agreements, groups must first answer a relatively simple question: where do international intragroup data transfers occur?

In principle, companies must already have a complete and up-to-date Record of Processing Activities (ROPA) which should already provide the key elements needed to identify international intragroup data transfers, including processing purposes, categories of recipients and any data flows involving third countries.

However, where documentation is incomplete or does not fully reflect operational reality, identifying intragroup transfers may require a more detailed assessment.

Many organisations rely on high-level data maps or organisational charts to identify international transfers. While useful, these tools frequently fail to capture the reality of intragroup access, particularly where:

- data is accessed remotely rather than physically transferred,
- multiple group entities interact with the same systems,
- functions are centralised but decision-making remains decentralised.

As a result, transfers integrated in everyday operations may remain invisible, despite being legally relevant.

From a regulatory perspective, the decisive factor is not how a function is labelled internally, but who can access personal data, from where, and under what conditions.

Key questions typically include:

- Which group entities have technical or organisational access to personal data?
- From which jurisdictions is that access exercised?
- Is access continuous, occasional or event-driven?
- Who determines the purposes and means of processing in practice?

Answering these questions often reveals transfer scenarios that are not reflected in existing documentation.

Why identification is particularly complex in intragroup contexts

Intragroup environments present specific challenges:

- overlapping roles between controllers and processors,
- hybrid models combining intragroup and outsourced processing,
- existing access rights that have evolved without formal review,
- and inconsistent documentation across jurisdictions.

For groups with a presence in Luxembourg, this complexity is often amplified by the central role Luxembourg entities can sometimes play in governance, compliance and oversight functions.

From identification to action: a strategic choice

While a high-level identification exercise can provide valuable insights, properly identifying and qualifying intragroup transfers requires a multidisciplinary approach, combining legal analysis, IT architecture review and operational input. This is precisely where many groups reach a tipping point: the exercise reveals enough risk to require action, but also enough complexity to make internal resolution challenging.

At that stage, ad hoc fixes or generic templates rarely provide sustainable solutions.

The identification of intragroup international data transfers is therefore not a box-ticking exercise, but a strategic governance decision. Groups that invest early in a structured and realistic assessment are significantly better positioned to implement proportionate safeguards.

5. Risks of not properly structuring IGDTAs in the current enforcement landscape

In this context, the risks associated with poorly structured intragroup data transfers have been intensified.

- **Regulatory risks**

Failure to properly structure intragroup international data transfers may result in findings of non-compliance with Articles 44 to 49 GDPR, corrective measures or administrative fines. In an environment of increased supervisory activity in this aspect, the inability to demonstrate compliance may itself constitute a breach.

- **Operational and governance risks**

Poorly documented intragroup transfers can undermine effective data governance, leading to unclear responsibilities, inconsistent incident handling and limited visibility over access rights.

- **Reputational and transactional risks**

In M&A transactions, financings or regulatory reviews, intragroup data transfer issues increasingly appear during due diligence. Deficiencies in this area may delay transactions, trigger remediation requirements or negatively impact evaluation.

6. Recommendations for organisations and their DPOs / privacy leaders

So how can organisations and DPOs move from identifying risks to actively managing them?

International intragroup data transfers are rarely the result of a single decision. They are usually the by-product of organisational choices, centralisation strategies and legacy access rights that evolve over time. For DPOs and privacy leaders, the challenge is therefore not only legal, but also organisational and governance driven.

Based on our experience, the following recommendations can help organisations move from blind spots to controlled and defensible intragroup transfer frameworks.

DPO Checklist

1. Shift the mindset: intragroup ≠ low risk

The first challenge is mindset. Many organisations still assume that intragroup data flows are inherently safer, even though regulators treat each legal entity as fully accountable. Recognising this gap is essential, because it is precisely where supervisory authorities increasingly identify weaknesses.

2. Identify and prioritise intragroup transfer risks

While a full technical mapping exercise may not always be immediately feasible, organisations should at least aim for a risk-oriented identification of intragroup transfers.

In practice, this means focusing first on:

- non-EEA entities with broad or permanent access rights,
- transfers involving sensitive data (employees, investors, whistleblowers),
- jurisdictions without an adequacy decision,
- and functions that operate across multiple entities and systems.

The real difficulty is not mapping what is known but uncovering what has never been formally assessed.

3. Strengthen accountability and documentation

Nowadays, the key question is not only “*Are we compliant?*” but also “*Could we prove it under investigation?*”

Authorities now expect organisations to demonstrate that their intragroup transfers are coherent, justified and aligned with operational reality. The challenge for DPOs is assessing whether the organisation can evidence this consistency. In many groups, documentation exists in fragments, making it difficult to comply with regulatory requirements without a structured framework.

This documentation plays a critical role not only during CNPD inspections, but also in the context of internal audits, regulatory reviews and transactions.

4. Treat intragroup transfers as a governance topic

Finally, intragroup data transfers should not be addressed solely as a contractual or legal issue. They are a governance topic that sits at the intersection of legal, IT, compliance and business functions. DPOs and privacy leaders are uniquely positioned to act as coordinators, ensuring that:

- legal requirements are translated into operational processes,
- responsibilities are clearly allocated across entities,
- and intragroup transfers are reviewed as part of broader governance and risk management frameworks.

In many cases, the governance model is not designed to capture cross-border access patterns, which is why external expertise becomes essential to build a sustainable structure.

These recommendations highlight that intragroup international data transfers are not a one-off compliance exercise, but an ongoing governance challenge. This leads directly to the question of what is at stake when such transfers are not properly structured.

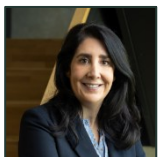
With this in mind, organizations that proactively address intragroup transfers are better positioned to avoid blind spots, withstand supervision by authorities, and ensure long-term operational resilience.

HOW WE CAN HELP

At **Stellan Partners**, our Technologies, Data & IP team assist clients in navigating these challenges by:

- Acting as external DPO / supporting internal DPOs
- Mapping and assessing intragroup data transfers.
- Drafting IGDTA and related documentation
- Supporting CNPD audits and due diligence
- Training teams internally

Please contact the members of our Technologies, Data & IP team if you would like to discuss how your organisation can better manage intragroup data transfers and meet GDPR requirements.



Audrey RUSTICHELLI

Deputy Managing Partner

New Technologies, Data & IP

audrey.rustichelli@stellanpartners.lu

T: +352 661 463 238



Mar IBÁÑEZ ARRIBAS

Associate

New Technologies, Data & IP

mar.ibanez@stellanpartners.lu

T: +352 621 164 754

This newsletter has been prepared by Stellan Partners for general guidance only. Although the greatest care has been taken to ensure that the information contained therein are accurate on the date of publication, Stellan Partners does not accept any liability to any person for the information (or the use or reliance upon such information) which is provided in this handbook or incorporated into it by reference. On any specific matter, please contact us for appropriate advice. The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.