# Navigating the increasing complexity of controller-to-controller terms

New privacy laws and frameworks impose more prescriptive controller-to-controller (C2C) terms. By **Nick Shepherd** and **Dan Cooper**, Covington & Burling LLP.

Over the past decade, companies across many sectors have grown accustomed to entering into data processing agreements with their vendors and suppliers that include certain provisions prescribed by law. Some sectoral privacy laws have imposed certain contractual rules for some time.[1] That said, a catalyst for making this a more widespread practice was the EU General Data Protection Regulation (GDPR), which went into effect in 2018. In particular, Article 28 of the GDPR sets out certain minimum contractual terms that must be included whenever a controller entrusts personal data to a processor (C2P terms). These terms have become even more commonplace in recent years thanks to emerging privacy laws in other jurisdictions (including state privacy laws in the United States), which include this same requirement for agreements between controllers and processors, and impose the same or similar core C2P terms.

By contrast, controller-to-controller privacy terms (C2C terms) have historically enjoyed more flexibility in comparison to C2P terms. This is due in part to the absence of an express legal requirement to have such terms in place (except in certain specific contexts), so such terms tend to be driven more by commercial considerations and a desire to lower potential legal exposure, as well as to satisfy broad accountability concepts. As a result, C2C terms can often take the form of high-level governance provisions between controllers – such as a commitment to each comply with applicable data protection laws; cooperate in good faith to support each other's compliance; implement baseline security measures; notify each other in the event of a breach affecting the shared data; and in some cases, agreeing to certain data use limitations or other bespoke provisions, depending on the context.

That said, new privacy laws and frameworks have gradually emerged which impose more prescriptive C2C terms in a range of scenarios. These can be organized into two main categories:

- The first category arises from nature of the relationship between the controllers – e.g., the rules for joint controller agreements set out in Article 26 of the GDPR, and the terms required by Section 7053 of the California Consumer Privacy Act (CCPA) Regulations for businesses that sell or share personal information with a third party.
- The second category stems from cross-border transfer rules. For example, Module 1 of the GDPR's standard contractual clauses (SCCs); the EU-US Data Privacy Framework (DPF) and its accountability for onward transfer principle; and more recently, the United States' Department of Justice's (DOJ) Data Security Program and its onward transfer prohibition on data brokerages with non-US recipients.

This article provides an overview of this increasingly complex landscape of C2C terms, to help companies take stock of their existing C2C agreements and any updates that may be needed, along with thoughts on key issues and potential risks to consider as part of that exercise.

## C2C terms stemming from the nature of the relationship

**GDPR rules for joint controller agreements:** Article 26 of the GDPR codified the concept of a "joint controllership," which arises when two or more parties jointly determine the purposes and means of processing personal data.[2] Such joint participation can be the result of a "common decision" or "converging decisions" about the purposes and essential means, which may lead to data processing that is "inextricably linked" due to the parties' pursuit of purposes that are closely linked or complementary.[3] Notably, in a joint controllership, one controller can be held jointly and severally liable with the other controller(s) for damages resulting from a violation of the GDPR.[4]

Where parties form a joint controllership, they must enter into an "arrangement" that allocates GDPR controller responsibilities between or among them – such as to provide notice to individuals, facilitate personal data rights, designate a point of contact, conduct data protection impact assessments (where applicable), and comply with cross-border transfer rules.[5] The GDPR further requires that joint controllers make the "essence of the arrangement" available to data subjects upon request, which the European Data Protection Board (EDPB) says should, at a minimum, "specify which [party] is responsible for [each of the controller obligations set out in the privacy notice]."[6] In addition, the EDPB advises that the arrangement should specify the parties' roles in communicating with supervisory authorities, such as in the event of a personal data breach.[7]

Due to the possibility of joint and several liability, as well as the added obligations described above, many companies have resisted the "joint controller" label and still do. To that end, it is not uncommon for C2C terms to include a provision whereby the parties explicitly agree that they are separate and independent (rather than joint) controllers. Moreover, as joint versus independent controllership can be an unclear or disputed issue, one way this sometimes gets resolved in negotiated agreements is to provide for both alternatives (e.g., "in the event the parties are independent controllers, then X"; "in the event the parties are joint controllers, then Y"). While this approach may leave room for ambiguity and differing interpretations, it may offer a compromise solution to move

negotiations along.

However, the EDPB and Court of Justice of the European Union (CJEU) have stated that contractual provisions alone are not determinative of a parties' processing role – so such a provision may be helpful, but is not risk-free.[8] In addition EU courts have more frequently called out joint controllership in recent case law.[9] Consequently, many companies subject to the GDPR may now be going through the exercise of examining whether their data sharing amounts to a joint controllership, and if so, considering how their C2C terms can be adjusted to meet joint controller requirements. This can be a meticulous and painstaking exercise, which specialist technical and legal support can help streamline.

**CCPA terms for selling or sharing personal information with third parties**: Under the CCPA Regulations, a business that sells or shares personal information with a third party must include certain terms in its contract with that third party.[10] At a high level, these terms must: limit the third party's use of such information to specific purposes, require CCPA compliance, grant the business oversight and remediation rights, and require the third party to notify the business if it can no longer meet these obligations.[11] The CCPA broadly defines a "sale" of personal information as essentially any disclosure of data by a business to a third party "for monetary or other valuable consideration," and "sharing" as any disclosure to a third party for "cross-context behavioral advertising" (CCBA) whether or not for monetary or other valuable consideration.[12]

Due to the potential risks and obligations associated with "selling" or "sharing" personal information under the CCPA, businesses often frame their data-sharing relationships in ways to avoid triggering sale/share obligations, or include terms to help mitigate sell/share risks. For example, disclosing personal information to a service provider falls outside the sale/share definition, so businesses will often impose service provider terms on counterparties wherever possible. However, in scenarios where this option is not viable (e.g., the data recipient is clearly not a service provider and/or will not agree to service provider terms), businesses must decide how to address the CCPA's third-party terms.

On the one hand, a business may be comfortable in its position that a particular disclosure to a third party does not involve CCBA or an exchange of data for any monetary or other valuable consideration. On the other hand, due to the broad concept of a "sale," there may be some residual risk of taking this position. Accordingly, some businesses may include a provision whereby the parties explicitly agree that the disclosure is not a sale/share under CCPA or other privacy laws – again, similar to the point above on joint controllership, such a provision can be helpful but is still susceptible to challenge. Another option some businesses employ is to be silent on whether the disclosure is a sale or share, but include all the third-party provisions required by the CCPA as a compliance backstop. These approaches and others come with pros and cons, and companies should carefully weigh these options in light of their data sharing activities and risk appetite.

## C2C terms imposed by cross-border transfer frameworks

**Module 1 of the GDPR's Standard Contractual Clauses**: The GDPR prohibits the transfer of EEA personal data to jurisdictions outside the EEA unless the transfer is to an adequate jurisdiction, or a valid transfer mechanism is in place, or there is an applicable derogation.[13] The SCCs are one such safeguard, and Module 1 of the SCCs should be used where both the EEA data exporter and non-EEA data importer are operating as controllers (whether jointly or independently).[14] Module 1 allocates GDPR-aligned obligations on in relation to transparency, purpose limitation, data minimization, security measures, and cooperation with supervisory authorities, and enables data subjects to enforce certain provisions as third-party beneficiaries. Importantly, the SCCs generally cannot be modified except for completing the annexes, and any substantive changes risk invalidating them.

In most cases, whether or not the SCCs are required is a relatively clear-cut analysis as set out above. That said, companies may need to negotiate certain aspects of the annexes, such as governing law and choice of forum for the SCCs, and align on transfer details. In addition, companies may need to negotiate obligations related to transfer impact assessments ("TIAs") in Clauses 14-15 of the SCCs, to evaluate whether the laws and practices of the destination country would undermine the protections in the SCCs, such that supplementary measures are needed for adequate protection. Thus, as with other C2C terms in this article, there may be significant compliance burdens and risk considerations triggered by these more prescriptive C2C terms.

**Onward transfer principle under the EU-US Data Privacy Framework**: The DPF is an adequacy framework under Article 45 GDPR which enables the free flow of EEA-originating personal data to DFP-certified US organizations.[15] The "accountability for onward transfer principle" requires such organizations to enter into a contract with any third-party controllers receiving onward transfers of the data (whether in the US or some other non-adequate country) that requires them to (a) process such data for limited and specified purposes, (b) provide the level of protection required by the DPF principles, (c) notify the DPF-certified entity if it can no longer meet this obligation, and (d) in the event of (c), cease the data processing or take other remedial steps.[16] EEA data subjects can bring claims against DPF-certified companies for failure to adhere to the DPF's principles.[17]

US companies certified to the DPF should review their agreements with any third-party controllers to whom they are onward transferring EEA personal data, to confirm these contractual terms are in place. In turn, any companies receiving onward transfers of EEA personal data from DPF-certified companies should bear in mind these use restrictions and their duty to comply with the DPF principles when handling such data, and their affirmative obligation to notify the DPF-certified organization if they cannot do so.

## Onward transfer prohibition under the DSP

The DOJ's data security program (DSP) is designed to address risks to

 

US national security, not to protect personal data or individual privacy interests.[18] In particular, the DSP is focused on preventing "access" (broadly defined) to certain types of government-related data and bulk US sensitive personal data by "covered persons" associated with certain "countries of concern" – i.e. China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela. The DSP includes the concept of a "data brokerage," which is broadly defined as "the sale of data, licensing of access to data, or similar commercial transactions […] involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data."[19] It encompasses a range of transactions that many businesses may not consider "brokering" transactions in the traditional commercial sense.

Among other things, the DSP requires US persons (e.g. companies) engaging in data brokerage transactions with non-US parties to contractually require the non-US party receiving the data to refrain from any subsequent covered data transaction involving the same data with a country of concern or covered person. The rule also requires the US person to report any known or suspected violations of this contractual prohibition to DOJ within 14 days. This aims to close "back-door" pathways whereby bulk US sensitive data could be resold, sublicensed, or otherwise transferred to covered persons or countries of concern indirectly.

US companies should check whether any of their transactions may qualify as a "data brokerage," and assess whether the data involved meets the DSP's definitions and bulk thresholds. Further, contracts with foreign counterparties that may meet this definition should include the onward transfer prohibition. Finally, companies should consider how this contractual term fits with broader contractual, oversight, recordkeeping, and reporting workflows involving third parties.

## Conclusion

As in-house legal and compliance teams continue to identify priorities for 2026, C2C terms may be an area that merits a closer look – especially for companies operating internationally, engaging in the types of data sharing described above, or as part of a broader refresh of contractual templates.

**AUTHORS**

Nick Shepherd, Associate in Covington's Washington, DC office, and Dan Cooper, Co-chair of Covington's Data Privacy and Cyber Security Practice (Brussels/Dublin).
Emails: nshepherd@cov.com
dcooper@cov.com

**REFERENCES**

1 See, for example, the US Health Insurance Portability and Accountability Act (HIPAA) and its rules for business associates agreements, in effect since 2003.
2 Article 26(1), GDPR.
3 See EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1 ("EDPB Guidelines"), paras. 54, 60.
4 Article 82(4), GDPR.
5 Article 26(1) GDPR, EDPB Guidelines para. 166.
6 EDPB Guidelines, paras. 180-181.
7 Id., paras. 190-191.
8 Id., para. 28. See also Case C-683/21.
9 See, e.g., Case C-604/22.
10 Cal. Code Regs., tit. 11, § 7053.
11 Id.
12 Cal. Civ. Code § 1798.140(ad) and (ag).
13 GDPR, Chapter V.
14 See Commission Implementing Decision (EU) 2021/914 of 4 June 2021. Also note that organizations outside the EEA, but subject to the GDPR, could in theory use the SCCs to transfer data. For example, a US company subject to the GDPR might need to rely on the SCCs to flow data to other parties, which can create a range of complexities to be resolved.
15 See www.dataprivacyframework.gov/ .
16 See DPF, Principle 3 ("Accountability for Onward Transfer").
17 See DPF, Principle 7 ("Recourse, Enforcement and Liability")
18 The DSP is codified at 28 C.F.R. Part 202 and has been in effect since April 8, 2025.
19 28 C.F.R. § 202.214


ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Towards better EU level cross-regulatory cooperation

The EDPS proposes to form Digital Clearinghouse 2.0. *PL&B*'s **Nel Anna Krzeslowska** reports on the future of possible cross-regulatory cooperation on new EU digital laws.

In recent years it has become evident that EU digital governance is no longer compartmentalised leading to an intersection between consumer protection, competition law, and data protection law, rendering siloed enforcement both inefficient and normatively inconsistent.[1] The GDPR, together with the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Act, and the AI Act form the EU's digital

*Continued on p.3*

# Driving data equity: Data sharing in the automotive sector

The EU Data Act has signalled a shift toward structured data access and reuse within the EU. The automotive industry is an example of data sharing resulting in innovation, but with consumers in mind. By *PL&B's* **Maisie Robinson**.

Data sharing is increasingly integral to multiple sectors, with the digital economy representing a substantial proportion of global GDP,[1] and cross-border data flows contributing trillions to economic activity.[2] Data is no longer merely an input; it is infrastructure.

Despite these developments, equitable distribution of the

*Continued on p.5*



Issue 200 **APRIL 2026**



**See the publisher's blog at privacylaws.com/blog2026apr**

INTERNATIONAL report

ISSUE NO 200 APRIL 2026

**PUBLISHER**
**Stewart H Dresner**
stewart.dresner@privacylaws.com

**EDITOR**
**Laura Linkomies**
laura.linkomies@privacylaws.com

**DEPUTY EDITOR**
**Tom Cooper**
tom.cooper@privacylaws.com

**ASIA-PACIFIC EDITOR**
**Graham Greenleaf**
graham@austlii.edu.au

**REPORT SUBSCRIPTIONS**
**K'an Thomas**
kan@privacylaws.com

**CONTRIBUTORS**
**Nel Anna Krzeslowska, Maisie Robinson**
*PL&B*
**Nick Shepherd and Dan Cooper**
Covington & Burling LLP, US and EU
**Graham Greenleaf**
Macquarie University, Australia
**Andin Aditya Rahman**
Assegaf Hamzah & Partners, Indonesia
**Hans Graux**
Time Lex, Belgium
**Nana Botchorichvili**
IDEA Avocats, France
**Wenlong Li**
Zhejiang University, China
**Yueming Zhang**
Ghent University, Belgium
**Annelies Moens and Caris Carroll**
Information Commission, Western Australia
**Andras Molnar, Urs Gasser and Markus Siewert**
TUM, Germany
**Sandra Cortesi**
Technical University of Munich, Germany
**Armando Guio Español**
Global Network of Internet and Society Centers
**David Dumont and Anna Pateraki**
Hunton Andrews Kurth LLP, Belgium

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
**Tel: +44 (0)20 8868 9200**
**Email: info@privacylaws.com**
**Website: www.privacylaws.com**

**Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative + 44 (0)7507 658880.
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X


# comment

## Children come at the top of the agenda

There is much emphasis on children's privacy now in the EU. Some Member States are looking into children's social media age restrictions, and the EU's Special Panel on Child Safety Online aims to present a report with recommendations to the Commission President by summer 2026. The UK government has the same timeline for a response to its consultation on children's digital wellbeing.

Meanwhile, the UK regulator fined Reddit £14.47 million for failing to properly check user ages and unlawful data processing. In the US, California's authority has recently taken action against PlayOn Sports, digital ticketing and media platforms for high school athletics and activities, resulting in a $1.1 million penalty.

The EU Digital Omnibus in currently being debated in Brussels. One of the main issues is the proposed changes to the personal data concept (p.8, p.19).

It looks like the AI Omnibus could be an easier task to accomplish (p.33). However, as digital regulation has expanded in recent years, questions remain how authorities from data protection, AI, competition and consumer protection could cooperate more effectively (p.1). Many structures are already in place. It remains to be seen how the EU Commission's AI Office will operate - one of the proposed measures in the AI Omnibus is to reinforce the AI Office's powers but that should not affect the powers and competences of the national authorities.

Read about GDPR fines and whether they are effective on p.22. Outside of Europe, we report on important developments in India (p.16), Indonesia (p.12) and Western Australia (p.27).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

## Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

# Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

## PL&B's International Report will help you to:

**Stay informed of data protection legislative developments in 180+ countries.**

**Learn from others' experience through case studies and analysis.**

**Incorporate compliance solutions into your business strategy.**

**Find out about future regulatory plans.**

**Understand laws, regulations, court and administrative decisions and what they will mean to you.**

**Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.**

## Included in your subscription:

**1. Six issues published annually**

**2. Online search by keyword**
Search for the most relevant content from all *PL&B* publications.

**3. Electronic Version**
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

**4. Paper version also available**
Postal charges apply outside the UK.

**5. News Updates**
Additional email updates keep you regularly informed of the latest developments.

**6. Back Issues**
Access all *PL&B International Report* back issues.

**7. Events Documentation**
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

**8. Helpline Enquiry Service**
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

**9. Free place at a *PL&B* event**
A free place at a *PL&B* organised event when booked in advance of the free-place deadline. Excludes the Annual Conference. More than one place with Multiple and Enterprise subscriptions.

**privacylaws.com/reports**

> *Privacy Laws & Business* is my go-to for the latest international thought leadership on hot topics in data protection law and policy.
>
> **Giles Pratt, Partner, Freshfields Bruckhaus Deringer LLP**

## UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data (Use and Access) Act 2025, the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

## Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.