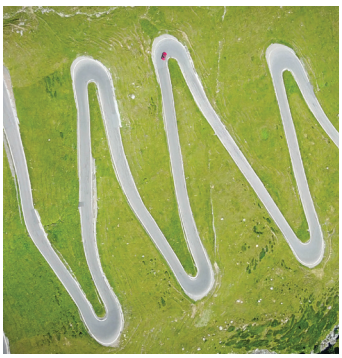
GDPR and consumer business supply chains



In our Future of Consumer series, we have previously explored how supply chain management is business critical in the consumer goods and retail sectors. Good management ensures that the right goods and ingredients get to market when they are freshest, when there is demand, in time for any promotions, and at the lowest cost. However, supply chains are also often engaged in relation to the processing of consumer data, including consumer preferences, purchasing history, financial and credit card details, and data analytics.

In a world where data is fast becoming a company's most valuable asset, engaging a service provider to process personal data on behalf of a company is commonplace. However, since 25 May 2018, the advent of the EU General Data Protection Regulation ("GDPR") has triggered specified regulatory requirements with respect to any commercial agreement involving the processing of personal data.

In this briefing we examine how these regulatory requirements with respect to data are resulting in commercial scrutiny of privacy provisions in supply chains as parties try to ensure that they are not left with a data liability gap. Further, where customer data analytics are being used to derive value, thorough due diligence will be needed throughout the supply chain together with robust data protection mechanisms.

The GDPR requirements

Under the GDPR, any company appointing a service provider to process personal data on its behalf is required to ensure that such service providers provide "sufficient guarantees" to implement appropriate technical and organisational measures so as to comply with the GDPR. There must be a written agreement between the controller and the processor and such agreement must incorporate the specific requirements set out in Article 28.

In the years leading up to the GDPR, it is fair to say that best practice for agreements involving personal data had evolved to include a range of supply chain protections from data breach notifications to controller rights to information or request compliance inspections. These provisions have now been elevated to mandatory legal requirements under the GDPR.

Impact of regulation on supply chain negotiations

Sub-processors: strengthening the supply chain

A combination of requirements under the GDPR together seek to ensure that clients retain control over personal data, even if the service provider wishes to sub-contract some or all of the processing to another entity. In addition, the original service provider cannot absolve itself of liability by using a sub-contractor.

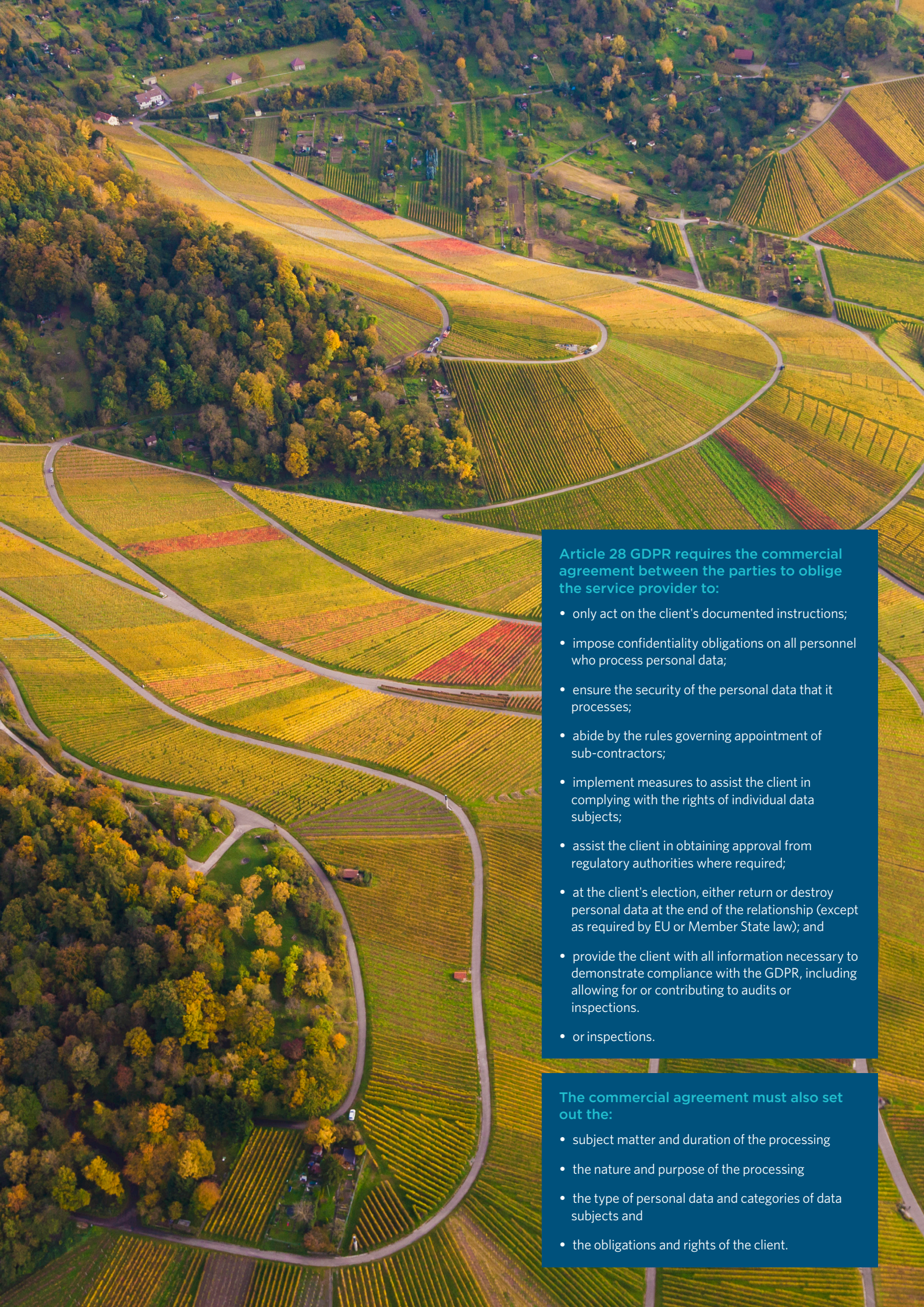
Under the requirements of Article 28, service providers are prevented from sub-contracting without the client's prior written authorisation, which can be general or specific. On the whole, clients are often unwilling to give general consents (e.g. a blanket consent to all sub-contracting) unless there are clear boundaries or conditions attached to that consent. However, if general consent is given, the service provider must inform the client of any changes in sub-contractors and give the client an opportunity to object. Whether it is realistic to seek such individual consent from the client for each change in sub-contractor will no doubt depend on the complexity of the supply chain and the practicalities of doing so.

Audit rights: an extension of the accountability principle

The GDPR requires service providers to allow for, and contribute to, audits (including inspections) conducted by the client or a chosen auditor of the client. It is worth considering the inclusion of any such provisions in light of existing information, record keeping or audit provisions in a commercial services/supply agreement. In negotiating these provisions it is also worth considering how prescriptive the audit process should be; how often is an audit permitted? At who's cost? What is the scope of the audit? Who should the auditor be and how should they be appointed? Can the client rely on the results of an audit carried out by the service provider? Again multi-tenanted platform service providers, in particular, tend to strongly resist audit rights due to by logistical challenges inherent in the nature of the services they offer; however parties may seek to compromise by using a jointly appointed or supplier-appointed independent third party auditor.

Security measures: what is appropriate?

A service provider is subject to the same security requirements as the client under the GDPR. It must take all measures required under the security provisions in Article 32 - namely to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing. The GDPR is not prescriptive as to what measures an organisation actually needs to implement to comply with this obligation, as this will need to be assessed on a case by case basis. Related challenges for negotiation in a supply chain context therefore include: what security requirements this obligation actually imposes in practice (taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of processing, as well as the risk associated with the loss or disclosure of personal data); whether the service provider needs to comply with detailed security requirements imposed by the client; and how parties can actually evidence compliance with these requirements.



Article 28 GDPR requires the commercial agreement between the parties to oblige the service provider to:

- only act on the client's documented instructions;
- impose confidentiality obligations on all personnel who process personal data;
- ensure the security of the personal data that it processes;
- abide by the rules governing appointment of sub-contractors;
- implement measures to assist the client in complying with the rights of individual data subjects;
- assist the client in obtaining approval from regulatory authorities where required;
- at the client's election, either return or destroy personal data at the end of the relationship (except as required by EU or Member State law); and
- provide the client with all information necessary to demonstrate compliance with the GDPR, including allowing for or contributing to audits or inspections.
- or inspections.

The commercial agreement must also set out the:

- subject matter and duration of the processing
- the nature and purpose of the processing
- the type of personal data and categories of data subjects and
- the obligations and rights of the client.

A service provider is also required to assist the client in ensuring compliance with its data breach notification requirements (both to the regulatory authority and the individual data subject), taking into account the nature of the processing and information available to the service provider. Once again, ambiguity remains over how much assistance is required by this obligation, whether "reasonable" assistance will suffice, whether the service provider should be entitled to charge for such assistance and whether this places additional regulatory responsibility on the service provider for the client's own compliance.

Gold-plating

Guidance issued by the UK regulatory authority (the ICO) re-iterates that the Article 28 provisions are very much a minimum set of terms; clients and service providers may wish to supplement them with additional processing provisions. Whilst clients continue to have more extensive liability than service providers under the GDPR, the former are still reliant on service providers to assist them in complying with their legal obligations. As a result, there are likely to be certain areas where clients require service providers to fulfil obligations that go beyond those set out in the Article 28 mandatory provisions, in order to comply with the GDPR.

It is often these "gold-plated" provisions that are the subject of most negotiation in commercial services/supply agreements as well as the related provisions addressing the respective risk allocation of the parties referred to below.

Risk allocation shift: emerging market practice?

Article 28 is silent on liability between the client and service provider. This is unsurprising given the bespoke nature of risk allocation between the parties and the need to balance and consider a variety of factors on a case by case basis, including the nature of the service provision and the relative exposure and mitigation measures available to each party. The liability regime falls outside the prescriptive mandatory provisions. However, we are now seeing a shift in the focus on, and related negotiation dynamic regarding, liability and indemnity protection. Whilst it will be some time before we are able to determine the approach to market practice, one thing is certain; liability regimes for breach of data protection provisions are being elevated in importance for both parties.

A position of uncapped liability for data protection breaches is definitely not market practice in the GDPR era. On the client side, clients are pushing for data protection breaches to be carved out of the overall liability cap; requesting high value "super caps" instead, in line with the higher penalties under the GDPR. On the service provider side, service providers are strongly resisting high caps for all but the most complex, high value and high risk agreements. This approach is reflected by requests from clients for more extensive contractual insurance obligations and a need for both parties to review the extent of their existing insurance coverage (including cyber liability insurance in the event of a data breach, given potential gaps in some traditional insurance policies).

In certain markets (particularly in the United States) we are also starting to see data loss being included as a specific head of loss under which a client is able to claim under its commercial services/supply agreement. As well as specific heads of loss being called out in the context of indemnities for data protection breaches (e.g. fraud prevention costs, breach notification costs).

Looking ahead: watch this space

Arguably the more prescriptive nature of the client/service provider relationship under the GDPR and the closer scrutiny warranted by both parties, is no bad thing for ensuring supply chain protection and further building trust and relationships with individual data subject. The GDPR makes it very clear that whilst risk can be outsourced to others in the supply chain, overall statutory responsibility cannot be outsourced.

The ICO currently prides itself on its "pragmatic and proportionate" approach to enforcement, with high fines being regarded a method of last resort. To date, the ICO has taken a light touch approach to investigating and enforcement action in respect of data processing arrangements as well. It remains to be seen whether this will continue once the GDPR applies, although we have already started to see closer regulatory scrutiny of complex data supply chains in the wake of the ICO's investigation into data analytics in political campaigns.

FMCG companies looking to derive significant value from their customer data through use of data analytics and complex supply chains will need to ensure that they undertake appropriate due diligence with respect to their suppliers and include appropriate and robust data protection provisions to comply with the GDPR.

This article is part of our **Future of Consumer series** on upcoming issues affecting the Consumer Sector. For other articles in this series see the Future of Consumer pages of our website or contact Rachel Montagnon

Rachel Montagnon
Consumer and IP Professional Support Consultant, London
T +44 20 7466 2217
M +44 7809 200 590
rachel.montagnon@hsf.com

Key contacts

Susan Black
Co-Head Consumer Sector Partner, London
T +44 20 7466 2055
M +44 7785 255 009
susan.black@hsf.com

Kristin Stammer
Co-Head Consumer Sector Partner, Sydney
T +61 2 9225 5572
M +61 414 957 572
kristin.stammer@hsf.com

Miriam Everett
Head of Data Protection and Privacy, London
T +44 20 74662378
M +44 7545 300 862
miriam.everett@hsf.com

Previous issues

Issue 1

The future of retail: AI, AR and VR

Issue 2

Targeted advertising

Issue 3

The supply chain and brand value

Issue 4

Targeting online risk

Issue 5

Bricks and clicks

HERBERTSMITHFREEHILLS.COM

BANGKOK
Herbert Smith Freehills (Thailand) Ltd

BEIJING
Herbert Smith Freehills LLP
Beijing Representative Office (UK)

BELFAST
Herbert Smith Freehills LLP

BERLIN
Herbert Smith Freehills Germany LLP

BRISBANE
Herbert Smith Freehills

BRUSSELS
Herbert Smith Freehills LLP

DUBAI
Herbert Smith Freehills LLP

DÜSSELDORF
Herbert Smith Freehills Germany LLP

FRANKFURT
Herbert Smith Freehills Germany LLP

HONG KONG
Herbert Smith Freehills

JAKARTA
Hiswara Bunjamin and Tandjung
Herbert Smith Freehills LLP associated firm

JOHANNESBURG
Herbert Smith Freehills South Africa LLP

KUALA LUMPUR
Herbert Smith Freehills LLP
LLP0010119-FGN

LONDON
Herbert Smith Freehills LLP

MADRID
Herbert Smith Freehills Spain LLP

MELBOURNE
Herbert Smith Freehills

MILAN
Studio Legale Associato in association with
Herbert Smith Freehills LLP

MOSCOW
Herbert Smith Freehills CIS LLP

NEW YORK
Herbert Smith Freehills New York LLP

PARIS
Herbert Smith Freehills Paris LLP

PERTH
Herbert Smith Freehills

RIYADH
The Law Office of Nasser Al-Hamdan
Herbert Smith Freehills LLP associated firm

SEOUL
Herbert Smith Freehills LLP
Foreign Legal Consultant Office

SHANGHAI
Herbert Smith Freehills LLP
Shanghai Representative Office (UK)

SINGAPORE
Herbert Smith Freehills LLP

SYDNEY
Herbert Smith Freehills

TOKYO
Herbert Smith Freehills