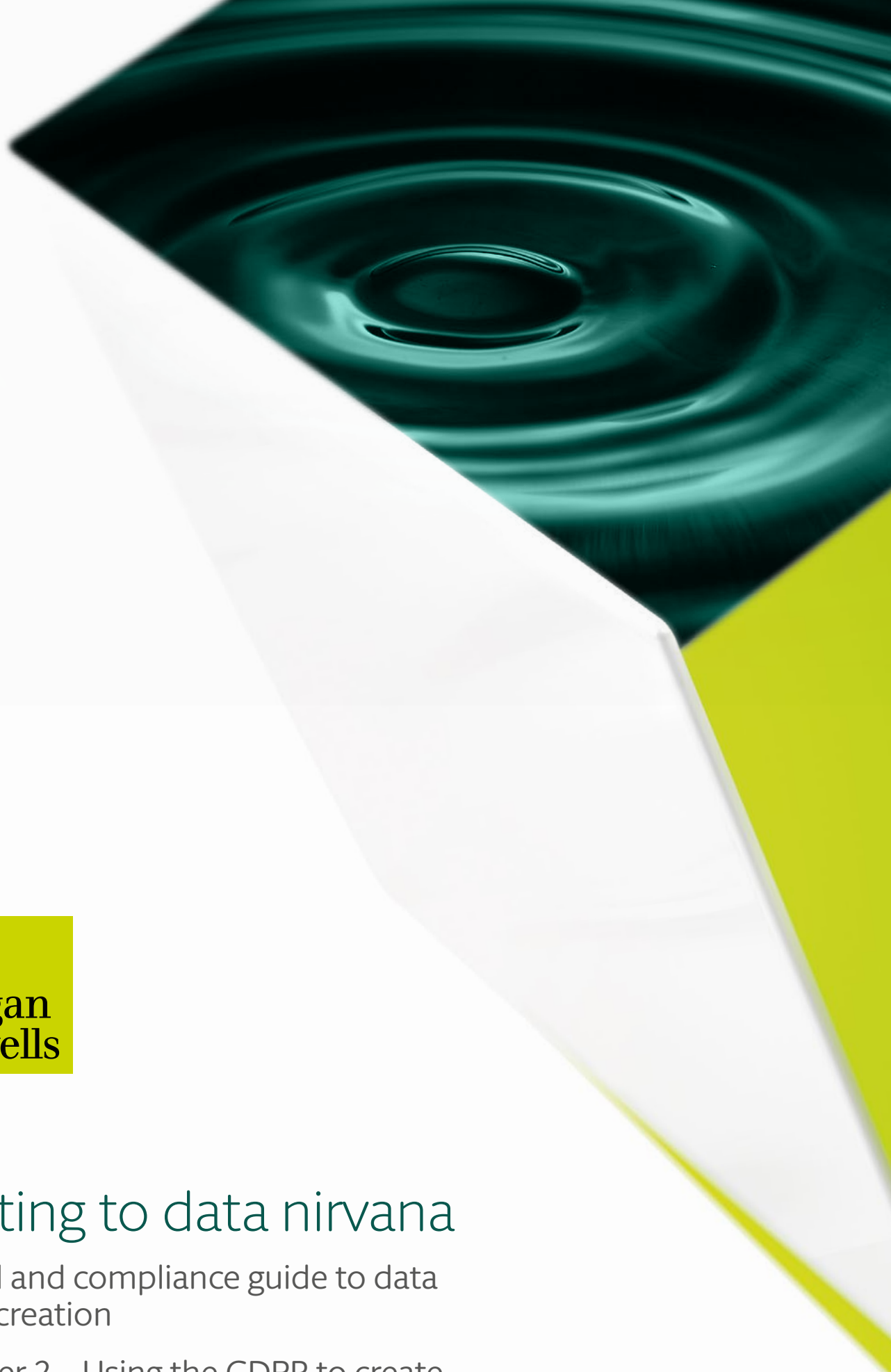


Hogan Lovells

Getting to data nirvana

A legal and compliance guide to data value creation

Chapter 2 – Using the GDPR to create data value

Winston Maxwell,
Partner,
Paris

Harriet Pearson,
Partner,
Washington, D.C.

John Salmon,
Partner,
London

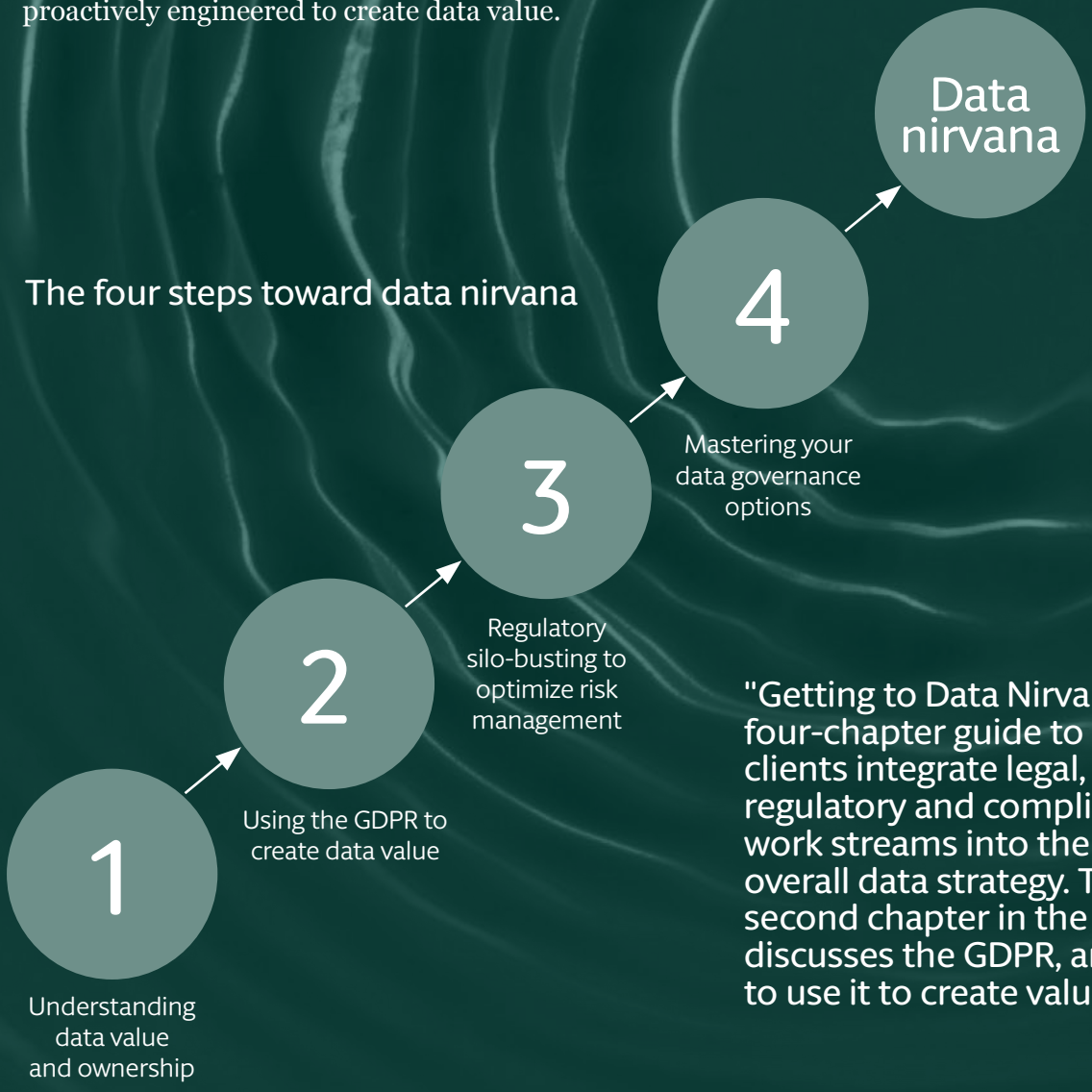
Eduardo Ustaran,
Partner,
London

Contents

Introduction

The job of legal and compliance teams is to make sure that their company's data projects don't violate applicable laws. Their task is not easy because laws regulating the processing of data – particularly data that is personal – are multiplying worldwide. However, a focus solely on data compliance can prevent broader thinking about data strategy, and how legal and regulatory teams can contribute to value creation.

Hogan Lovells' "Getting to data nirvana" guide helps open the door to broader thinking about data strategy, by showing how regulatory, contract, IP, competition and litigation strategy can be proactively engineered to create data value.



"Getting to Data Nirvana" is a four-chapter guide to help clients integrate legal, regulatory and compliance work streams into the group's overall data strategy. The second chapter in the series discusses the GDPR, and how to use it to create value.

Chapter 2 – Using the GDPR to create data value

1. GDPR Tools can be re-purposed to contribute to data value

Like many regulatory constraints, data protection rules limit what an organization can do with the data, thereby reducing data's utility and value. Nevertheless, the GDPR[1] requires organizations to put into place mechanisms that paradoxically can be used to increase data value. Those mechanisms include:

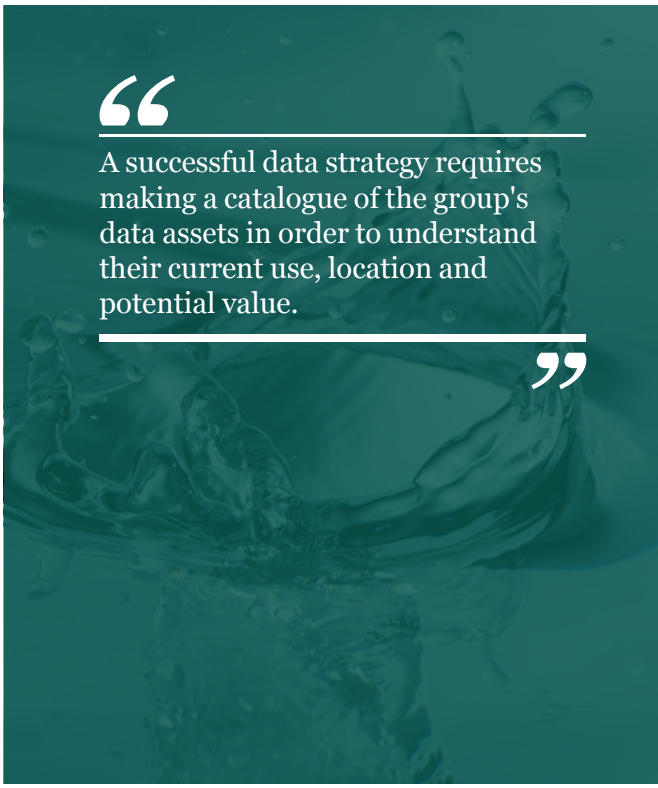
i) the creation of a comprehensive mapping and record of data processing,

ii) the requirement of data processing and data transfer agreements,

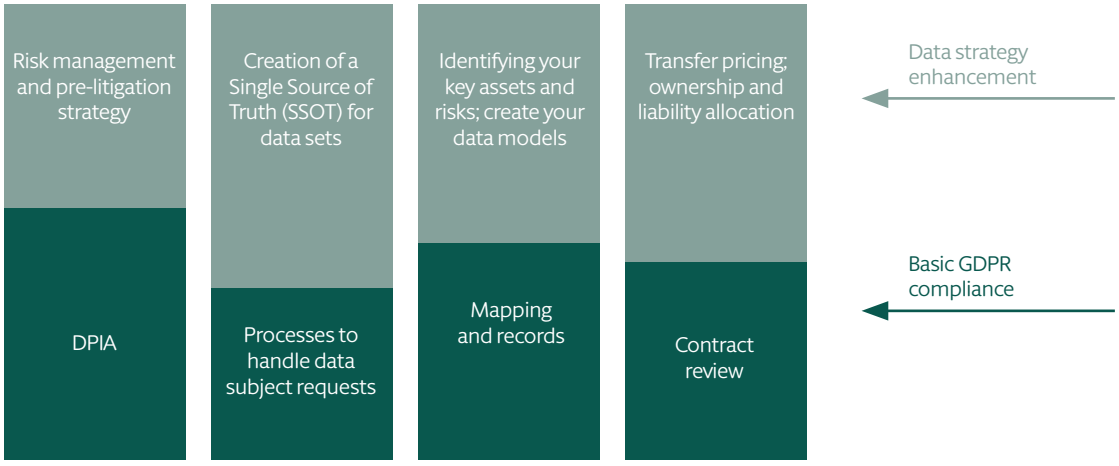
iii) data protection impact assessments, and

iv) the requirement to create a mechanism – what data managers call a "single source of truth" (SSOT) -- to handle data subject access and rectification requests.

Each of these mechanisms is designed to enhance data protection but each can also be used to enhance data value.



Using GDPR to Create Data Value



> Is your company creating a data catalog so that all data assets are known?
>
> *J. Short and S. Todd, 2017*

2. Data mapping and GDPR data records

A successful data strategy requires making a catalogue of the group's data assets in order to understand their current use, location and potential value.

The GDPR also requires a comprehensive mapping of data processing operations involving personal data, and the creation of a data processing record, albeit for totally different reasons. For the data manager, the reason for mapping is to locate assets that can be managed. For the data protection officer, the reason for mapping is to ensure compliance with the GDPR. The GDPR data record must list the kind of personal data processed, the purposes of processing, the legal basis for processing (e.g. consent, legal obligation, of legitimate interest), recipients of the data and the existence of transfers and data processors. The record must identify which entity or entities in the group are responsible for the processing operation as "data controller," and which entities are merely following instructions and processing data on behalf of other entities as "data processors." Identifying which corporate entity is the data controller[2] of data within the group is an indispensable first step to optimizing value, and may create opportunities for improving the internal group structure for data handling (see Section 3.2 below on intragroup agreements and transfer pricing). As explained in chapter 1, the data controller is the functional "owner" of the data. The controller has duties to the data subject, but also acts as gatekeeper and principal beneficiary of data uses.

Identifying the purposes of data processing in the GDPR data record also permits organizations to attribute values to different data sets and uses. This kind of value mapping is a critical first step to developing a global data strategy, and also comes in handy for corporate transactions and cyber-security audits, where the data most valuable to the business needs to be identified and located. The creation of a GDPR record therefore pushes organizations to do something they should be doing anyway under good data management principles.

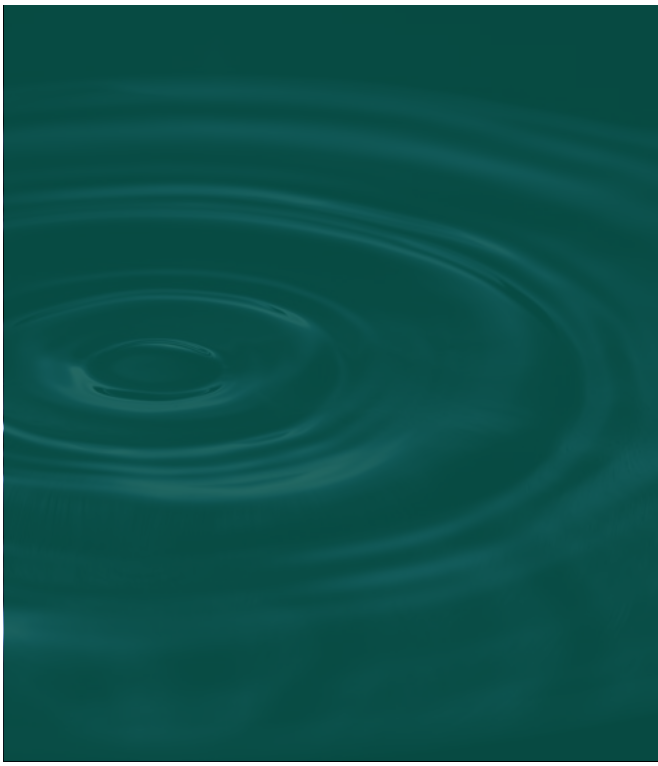
3. Intra-group data agreements

The GDPR requires that data transfers be documented through **data transfer agreements.** When an entity processes data on behalf of another entity, this must be documented in a data processing agreement. Shared responsibility over data must be documented in a **joint controller agreement.** These data agreements, which we call "GDPR contracts", are often entered into between companies in the same group. These contracts provide an opportunity to allocate ownership rights and liability among companies in the group and implement transfer pricing.

3.1 Structuring intra-group contracts to allocate liability and maximize value

GDPR contracts present an extraordinary opportunity to clarify and improve the data processing structures and contracts within a group, as well as contracts with the group's main commercial partners. A successful overhaul of internal data contracts and structures should not be driven solely by GDPR compliance. Consideration should also be given to liability sharing, where the economic value of the data should be located in the group, and how contractual structures can be optimized. For example, for most banks, the owner of customer data -- the data controller -- will be the local retail entity with whom the customer has a banking relationship. The processing of the customer data may then be performed by a central IT entity in the group, acting as data processor for the retail entity. However, the central IT company may in fact be doing more than just processing data for the relevant retail entity. The IT company may also be analyzing transaction data to detect potential fraud, or to monitor risks under the group's risk reporting system.

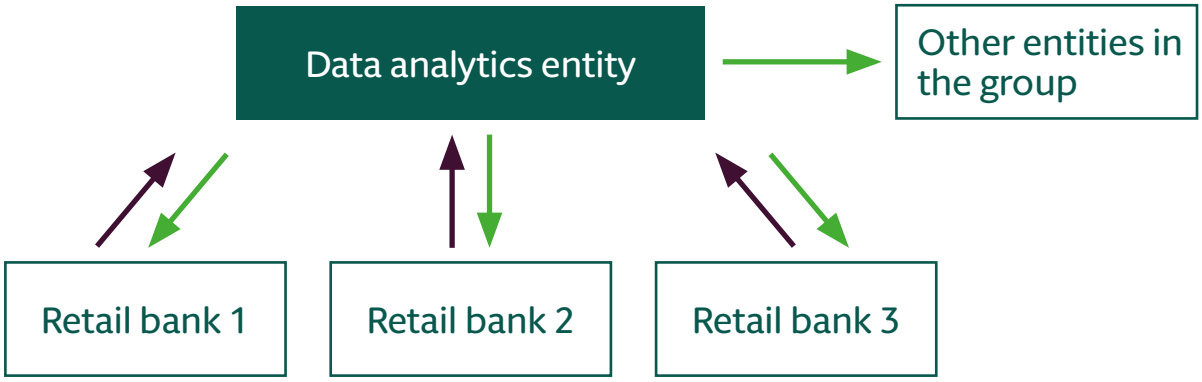
“Contracts provide an opportunity to allocate ownership rights and liability among companies in the group and implement transfer pricing.”



There also may be data analytics that feed into a central anti-money laundering and terrorist financing surveillance system. Finally, there may be analysis of customer data -- or an anonymized version thereof -- to help the group understand geographic and demographic trends that will help the group better understand churn or develop new services.

The IT processing company will be creating value for the local retail entity for which it is processing data, but will also be creating value for the group as a whole by sharing data analytics insights. Some of the new value created might even come from selling data insights to entities outside the group.

The GDPR, or rules on bank secrecy, may limit the ability to conduct detailed analytics, particularly of transaction data. However, the point in this example is that a group should consider where the additional value created from data analytics should be located within the group, i.e. which entity or entities should be considered the owners of these valuable new insights.



Green arrows = benefits from data insights shared with other companies in the group

Purple arrows = raw data sent for analysis

3.2 Transfer pricing

The contractual structure will also be influenced by tax and transfer pricing considerations.

Tax authorities are seeking to understand where data value is located within groups, including where data are collated or analyzed, and where the insights of data analytics are being used for other value-adding purposes. Tech companies already face this challenge in tax and transfer pricing audits, and companies in other sectors will be next. Banking and insurance may be a new area for tax authorities to focus on once data analytics for financial services firms start creating significant value. There may also be opportunities, especially where data projects permit the structuring of data transfers and value creation within the group, as well as cost-savings.

A threshold question in transfer pricing is to determine where the "value" is. Is the value in the data or the algorithms? Then how do we price the relevant services or insights that result from data analytics? Is there a fair market value? Whenever value is created and shared within a group, transfer pricing should be implemented based on the fair market value of the service or insights that are being shared. Where there exists no market price for the internal data services, the group should look to prices of comparable services, such as those of third party data analytics or brokerage services.

The review of data flows and contracts required by the GDPR presents a unique opportunity to address these questions, which will have crucial importance as the value of data within the group grows.

“A threshold question in transfer pricing is to determine where the "value" is.”

> The data protection impact assessment is an opportunity not just to address data risks, but to explain the value proposition associated with the data project.

4. Data protection impact assessments permit a holistic approach to risk mitigation

The GDPR requires the preparation of data protection impact assessments for operations that are likely to create a high risk for individuals.[3] Many kinds of data analytics performed on customer data could satisfy this "high risk" test.[4] The impact assessment is intended to foster an understanding of the underlying risks and different mitigation options that can be deployed to reduce the risk. The objective of the impact assessment is to identify risk mitigation steps that bring the risks to an acceptable level, while still, if possible, preserving the utility of the underlying data project.

The data protection impact assessment is an opportunity not just to address data risks, but to explain the value proposition associated with the data project: the benefit for the organization, for users and for society. This review of the total benefits will affect the risk-benefit analysis, and the decision on what level of data protection measures are "appropriate" with regard to the risk and the context.

The data protection impact assessment is also the ideal opportunity to apply the regulatory silo-busting explained in Chapter 3 below. For example, when evaluating appropriate data security measures under Article 32 GDPR, the impact assessment would also integrate security and other requirements under other regulations, such as, in the banking field, PSD2, MiFID II, the 4th AML Directive and the NIS Directive. A data protection impact assessment that **only** addresses GDPR requirements is a missed opportunity to implement a more holistic approach to risk mitigation where different security requirements overlap.

Finally, a well-built impact assessment will help preserve the value of data by protecting against lawsuits later on. Under the GDPR's system of accountability, an organization must demonstrate compliance, and in particular that it has implemented appropriate technical and organizational measures. The data controller will have the burden of proving that the measures it took were "appropriate." The only way to do this, absent detailed technical standards, is to produce a data protection impact assessment analyzing the various technical and organizational measures and choosing the one that presents the optimal tradeoff between protection and utility.

5. GDPR and the "single source of the truth" (SSOT)

By giving data subjects an enhanced right to access, rectification and erasure, the GDPR will force data controllers to develop a single interface for dealing with such requests, as well as a single source of truth (SSOT) for consumer data. A correction made by the data subject to his or her data must be propagated into all the group's systems and data silos. For large incumbent firms with multiple data silos and applications, this can be a daunting task. However, generating this sort of feature, which data managers call a "single source of truth" or "SSOT", is also essential for any data strategy. The process can be costly and labor intensive. But it is a critical first step to extracting value from heterogeneous data sets.

Here again, GDPR compliance aligns perfectly with big data value creation. The GDPR work stream on individual data access rights needs to be integrated into the SSOT data work stream, assuming one exists. Otherwise, two teams will be working in silos, trying to address the same problem but from different angles, the GDPR compliance angle and the value creation angle. The two approaches should be merged.

> The SSOT is a logical, often virtual and cloud-based repository that contains one authoritative copy of all crucial data, such as customer, supplier, and product details….Not having an SSOT can lead to chaos. One large industrial company we studied had more than a dozen data sources containing similar supplier information, such as name and address. But the content was slightly different in each source.
>
> *Leandro DalleMule and Thomas Davenport, 2017*

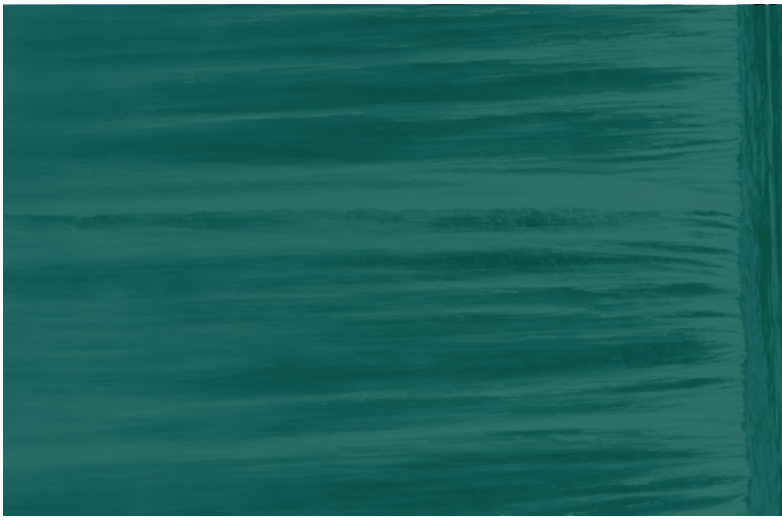
6. Summary of GDPR tools that can be re-purposed to enhance data value

The following table summarizes the beneficial overlap between GDPR and steps needed to create a successful data strategy:.

	Tools necessary for a successful data strategy	Tools required under GDPR
SSOT	SSOT is one of the most critical and expensive aspects of most data lake projects.	Under GDPR, a mechanism is required handle data subject access, rectification and erasure requests and make sure that all data in legacy data silos are covered.
Data mapping	A catalogue of data is critical to a data strategy.	Under GDPR (article 30), data controllers must create detailed records and mapping.
Data contracts	Data contracts can help locate data value and liabilities with the right entity in the group.	Data processing, joint controller and data transfer agreements are required under Articles 26, 28 and 46 GDPR
Transfer pricing	Data contracts need to reflect transfer pricing rules.	Not required under GDPR, but a recommended by-product of data processing and transfer agreements.
Impact assessments	Impact assessments present an opportunity to look at data risk-mitigation measures in the whole, taking all regulatory constraints into account, not just GDPR.	DPIAs are required under article 35 GDPR for all risky processing. DPIAs are an essential tool to protect against liability.

References

1. European General Data Protection Regulation 2016/679.
2. We use the term "owner" to mean the entity that holds whatever usage rights the group has with respect to the data, taking into account contractual and regulatory constraints.
3. Article 35, Regulation (EU) 2016/679.
4. Article 29 WP Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 4 April 2017 as last revised and adopted on 4 October 2017, WP 248 rev.01.



Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices