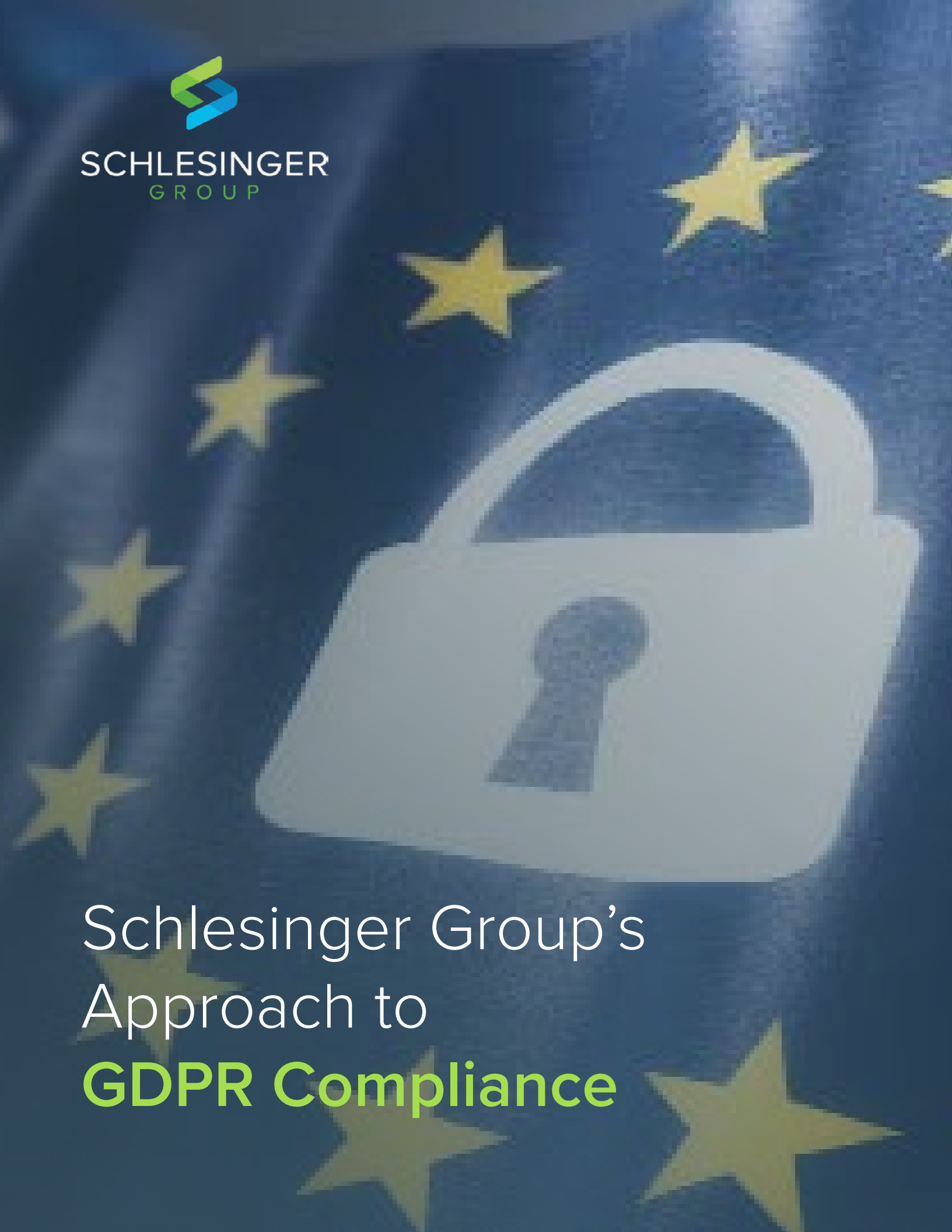

SCHLESINGER
GROUP

Schlesinger Group's Approach to **GDPR Compliance**

Schlesinger Group is trusted by its clients to conduct quantitative and qualitative data collection studies within GDPR guidelines. Since the Regulation came into place in 2018, we have conducted thousands of studies in Europe, guiding our clients through the GDPR landscape. Where a project may be unusual or particularly complex, our legal expert on retainer consults with us to ensure compliance while meeting your research needs.

SECTION 1:
A short guide to GDPR

What is GDPR?

The EU General Data Protection Regulation (GDPR) is a new regulation that replaces the 1995 EU Data Protection Directive. It sets new standards for the collection, use, processing and transfer of the personally identifiable information (PII) of European Union citizens. Significant and wide-reaching, the new law brings a 21st Century approach and fundamental rights for European Union citizens living in the digital world.

When was the Regulation effective?

May 25th 2018. Previous national data protection regulations in EU were replaced by GDPR.

What is the reach of GDPR?

It applies to all European Union member states and also any country or entity that transfers the personal data of EU citizens outside of the European Union.

What is the objective of GDPR?

General Data Protection Regulation provides a single set of rules for data protection across Europe.

Firstly, GDPR seeks to expand the rights of individuals over how organizations use their personal data and to bring data protection law in line with how people's data is being used. The internet and the cloud have allowed organizations to develop methods to use (and abuse) personal data. GDPR aims to control this by placing new obligations on organizations to be more accountable for data protection.

The second driver is the EU's desire to making data protection law identical throughout member states to give organisations more clarity over how they can behave.

Is the law consistent across all EU countries?

Multiple exemptions allow members states discretion. Some articles will be defined differently from country to country: Notably, for market research purposes;

Article 8, concerning child age of consent

Article 9, concerning storing of special data categories, such as health conditions

Even where some flexibility of clauses is given, it is very limited and much specified.

How does GDPR regulation age of consent vary between European countries?

Not all consent ages have been finalized. The latest information (May 2018) indicates:

Age 13:	Czech Rep., Denmark, Finland (Ministry of Justice recommends either 13 or 15), Ireland, Latvia, Poland, Spain, Sweden, UK
Age 14:	Austria
Age 15:	Greece
Age 16:	France, Germany, Hungary, Lithuania, Luxembourg, Netherlands, Slovakia

How does GDPR relate to Privacy Shield?

The Privacy Shield Framework only addresses the data transfer requirement. US companies, like any companies in the EU, must comply with all the requirements of GDPR when collecting personal data.

How does GDPR relate to Brexit?

The UK **Data Protection Act 2018** came into force in May 2018. It is the UK's implementation of **GDPR**. However, GDPR is only a part of the overall UK data protection framework. GDPR gives member states limited opportunities to make provisions for how it applies in their country. One element of the DPA 2018 is the details of UK provisions. It is therefore important that the GDPR and the DPA 2018 are considered together.

Does the Regulation apply to Anonymized data?

No, if the data collected is anonymized, GDPR does not apply for your study. Thus, If Schlesinger Group, as the controller provides sample, conducts fieldwork and delivers anonymized data, then GDPR is irrelevant to the client.

What constitutes personal data?

GDPR expands the definition of personal data. What constitutes 'personal data' is much broader and it specifically covers 'online identifiers'. Personal data is all information linked to a person. This is primarily the contact details but personal data is also any information that can be used to directly or indirectly identify the person. We advise our clients to be clear on what is classed as personal data.

Identifiable information such as

- name
- address
- IP address
- photo
- audio & video recordings
- email address
- bank details
- online behavior: cookies, posts on social networking websites.
- device IP address
- mobile device ID

Profile/sensitive/special category information such as

- household information,
- behaviour and attitudes
- medical information
- health conditions
- ethnicity
- religion
- trade union membership
- sexual orientation
- political attitudes
- biometric data
- genetic data

What is the difference between a data controller and a data processor?

GDPR places obligations on a data controller and a data processor.

A **data controller** is an entity that determines the purposes, conditions and means of the processing of personal data.

A **joint data controller** is two or more entities that jointly determine the purposes and manner in which data is used.

A **data processor** is an entity that processes personal data on behalf of the controller.

In which cases is the end client considered an observer (and not the controller)?

We consider as “Observer” any third party who

a. has no access to personal data

b. has not determined the design/methodology of the study but has only defined the objectives of the study or the broad research question

c. has not provided any specific detailed guidelines, questionnaires or sample, such as client lists.

We are not required to reveal the identity of the Observer but we are required to reveal the Observer ‘Category’. This is revealed during recruitment and/or when obtaining consent in facility/on-site.

In which cases is the end client considered (joint) controller?

When the End Client

a. receives personal data (including video without names) to be stored and not just observed

b. and/or has determined the study details

Then we consider the End Client to be Joint Controller, together with either the company conducting the data collection or the research agency.

SECTION 2:

Compliance for the collection, usage, processing and transfer of personal data in relation to marketing research services at **Schlesinger Group**.

How compliant is Schlesinger Group with GDPR?

- We have invested and continue to invest in legal advice for reliable interpretation of the legislation for our businesses
- We are conducting a data protection impact analysis (DPIA)
- We have reviewed and continue to review the data we hold and our data process
- We have updated our privacy policies
- We have appointed Data Protection Officers (DPOs) in each of our countries.
- We have addressed requirements relating to obtaining consent, including child age of consent for the countries in which we operate
- We have addressed our ability to provide personal data information upon request and the right to be forgotten and data portability
- We have addressed data protection by design and default
- We have addressed data transfer out of the EU
- We have addressed the issue of risk
- We have prepared a data breach notification process
- Robust data protection technology is already in place

Who are the Schlesinger Group DPOs?

USA - Schlesinger Group
Howard Schlesinger
Howard.Schlesinger@SchlesingerGroup.com

UNITED KINGDOM - Schlesinger Group UK
Sara Spicer
Sara.Spicer@SchlesingerGroup.com

GERMANY - - Schlesinger Group Germany
Christian Holdt
Christian.Holdt@SchlesingerGroup.com

SPAIN - - Schlesinger Group Spain
Ana Cañas
Ana.Canas@SchlesingerGroup.com

FRANCE - Schlesinger Group France, Passerelles & Vigie Pharma
Fadila Vargas
Fadila.Vargas@VigiePharma.fr

What is the role of our DPOs?

All Schlesinger Group companies have a local Data Protection Officer (DPO) with whom you can connect if you consider your project may have implications for GDPR. Our DPOs will also step in, as requested by our Project Managers, for advice on GDPR compliance.

For multi-national projects in Schlesinger EU countries, local DPOs collaborate, under the supervision of the European Operations Director, to offer a one-stop data protection solution. Our local DPOs review projects to ensure projects also comply with other local country regulation.

Local DPOs can advise on clients confidential agreements to help comply with the GDPR and ESOMAR guidelines.

How Schlesinger addresses transparent and clear research participant consent?

In all Schlesinger European participant panels the new conditions for consent are being renewed.

Requests for consent are given in an intelligible and easily accessible form, with the clear purpose for data processing attached to that consent.

Consent is clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. For the panel but also for special consents on projects, we make it as easy to withdraw consent as it is to give it.

Addressing data access and portability

Under, GDPR, Schlesinger Group panelists and respondents have the right to see everything stored on them as a person and the right to have this exported to them. We are able to fully support such requests.

Addressing the right to be forgotten

Under GDPR, our panelists and respondents have the right for all of their personal data to be erased from the project and systems.

This right is covered with our database routines that perform this task on time-based requests. In relation to personal information transferred to processors for Schlesinger Group, Schlesinger Group has a contractual process for the processor to also delete such personal information upon request.

Addressing data protection by design & default

Our internal developed tools working on PIIs and personal data have previously been designed and built in way that meets GDPR standard and have been approved externally.

Where Schlesinger Group uses third party software and services that work on PII and personal data, partners will need to prove GDPR conformity in order to become a Schlesinger Group partner.

Addressing a base for data transfer out of the EU

We deploy a multi-step framework with regulations specified by the EU for internal company data transfers.

1. Firstly, the Legal basis to allow data transfer will be project-based consent of respondents, including the foreseen transparency.
2. Then, we analyze the country to which the data transfer is to be made to assure an adequate level of data protection.
3. Thirdly, we provide a framework contract between the controller (ultimately responsible for data) and the processor (receiver of the data) ensuring that the level of data protection in non-EU countries applies to the definitions and foreseen mechanism of the EU. Where appropriate, our DPOs assist setting up a legal framework, including Confidentiality, Non-Disclosure Agreements and other documents mandated by laws and regulations such as the Privacy Shield and the EU Standard Contracts.

Assessing risk

Based on the library of data processes on personal data, all procedures used by the Schlesinger Europe Companies are determined by reference to the nature, scope, context and purposes of the data processing, including the receipt and protection of personally identifiable information, profile, sensitive data and special category information. Risk is evaluated on the basis of an objective assessment for each project, through which the nature of the data processing risk is established.

Who is the Controller? Who is the Processor? - Our definitions, in line with the GDPR and various European associations and authorities:

The GDPR regulation mentions 'Controllers', 'Processors' and 'Recipients' in the definitions of roles, responsibilities. It prescribes when, how and to which extent the subjects (respondents) should be informed of such roles as part of the research process.

Below are some typical examples of how Schlesinger Group is approaching data roles and their identification in our studies:

1. Schlesinger project managing or recruiting on a client list only

CONTROLLER = Client (Research Agency/ End-Client/Sponsor)	PROCESSOR = Schlesinger

- If the Controller does not present their own Controller-Processor agreement, then the Schlesinger DPO will provide a standard agreement template.
- Schlesinger will use the client list according to client instructions.

Controller Identification

- Respondents must be informed of the research agency identity during the recruitment process. Any other stakeholders can be revealed as a 'category'.
- In the case where the End Client is Controller, the conducting marketing research agency is responsible for revealing the name of the client after the interview.
- At any time in the process, upon respondent request, the identity of the Controller must be revealed.

2. Schlesinger project managing or recruiting on a client list & Schlesinger panels.

CONTROLLER = Client (Research Agency/ End-Client/Sponsor)	PROCESSOR = Schlesinger for client list usage	CONTROLLER = Schlesinger for own Panel for PII transfer

- If the Controller does not present their own Controller-Processor agreement, then the Schlesinger DPO will provide a standard agreement template.
- Schlesinger will use the client list according to client instructions.
- Additional respondents will be recruited from the Schlesinger panel and, if necessary, consent will be obtained for transfer of any PII required for the study. Schlesinger will provide a short agreement for PII transfer from Controller-to-Controller.

Controller Identification

- See Example 1.

3. Schlesinger project managing or recruiting via Schlesinger panels with recordings to the marketing research agency only.

CONTROLLER = Client (Marketing Research Agency)	CONTROLLER = Schlesinger for own Panel for PII transfer	OBSERVER = Does not receive PII or recordings at all

- End client /sponsor is considered by us as the Observer only – we do not define them as Controller
- Schlesinger will provide a Controller-to-Controller agreement in which we define the usage and limitations of video recordings.

Controller Identification

- The GDPR requirement for transparency is to name as Controller the marketing research agency receiving personal data and conducting analysis of the focus groups/IDIs and the video recordings.
- Observing clients who are not defined as Controller are not required to be named after the interview. In this case, we consider the role of Observer to be appropriate.
- The End client may demand the role of Controller, in which case all GDPR responsibilities for protection of PII and transparency of roles remain wholly with the client.

4. Schlesinger providing the facility and recordings only

CONTROLLER = Client (Research Agency)	PROCESSOR = Schlesinger Client Service

- In this case, the client, as Controller holds all responsibility for GDPR compliance. That is; to obtain consent for participation, for the storing of personal data and recordings, and possibly for the transfer of such data.

Controller Identification

- The client is also responsible for providing the required transparency for the respondents, depending on the role of their client (Controller or Observer).
- Schlesinger will work directly on behalf of the client, e.g. on boarding and seating the respondents, gathering signatures for the clients' consent forms, incentive handling, conducting recordings, passing the recordings to individuals, as directed by the client.
- Usually all documents should be provided by the Controller. Where this is not the case, Schlesinger will make available all necessary documentation in an unbranded format for use by our clients for 'room rental' work.

5. Schlesinger project managing or recruiting on Schlesinger panels with external recordings / visits

CONTROLLER = Client (Research Agency)	CONTROLLER = Schlesinger for own Panel for PII transfer

- Schlesinger will provide a Controller-to-Controller agreement in which we define the use and limitations of PII and self-recording rights.
- Schlesinger will obtain the consent for personal data to be transferred to the client as 2nd controller.
- The 2nd Controller is fully responsible, in terms of GDPR, for the data evaluation.

Handling breach notifications

Under GDPR, our process is in place so that:

1. The Processor shall notify the Controller as soon as possible after becoming aware of any personal data breach.
2. Any breach of data protection will be reported to the identified national Data Protection Authority by the data Controller within 72 hours.
3. If the breach is considered a high risk by GDPR definitions, the affected respondent will be informed.

Anonymizing personal data for your studies

Anonymizing personal data is already the usual case for Schlesinger Group and responsible data collection and research companies in Europe. As such, any project data is already being shared strictly anonymously.

We can give our clients very detailed information about a respondent as long as it is not connected to an identifiable person. To avoid any risk to your company, the ideal is not request personally identifiable data. And this should not have a big impact as the data you need for your results does not need to be identifiable.

Managing exceptions responsibly

In special situations such as for IHUTs, ethnographic interviews, or shared recruitment solutions, personal information needs to be shared to conduct the study effectively.

For such projects, information is separated so that only necessary data is shared. For each case, the respondents need to accept additional consent for the information to be shared for the project.

If personally identifiable data is considered to be needed, we will endeavor to provide it within the law. However, at this point, the client/partner receiving the personal information becomes liable to meet GDPR regulations - with all the new increased rights of the respondents in Europe.

Please note: This document does not supply legal or procedural advice for any company's GDPR compliance.

Further information regarding GDPR compliance when working with Schlesinger Group

For conversations regarding a particular study, please contact
the national Schlesinger Group DPO listed on page 9

For general conversations regarding GDPR, please contact
Christian Holdt | Director, Operations, Schlesinger Europe
Christian.Holdt@SchlesingerGroup.com

For conversations regrading compliance for any other matter, please contact
our Compliance Team at Compliance@SchlesingerGroup.com

Additional resources

(Europe) ESOMAR Data Protection Checklist

(USA) Insights Association: GDPR Portal

(UK) Market Research Society: GDPR In Brief Series

(UK) Information Commission Office

Further information

Christian Holdt, Director Operations
Schlesinger Europe
Christian.Holdt@SchlesingerGroup.com