STRÖER

DATA PROTECTION

CONTENTS

01

Introduction

The data protection management system (DPMS) was set up for the Ströer Group taking into account generally accepted standards, applicable law and individual company requirements depending on the type and scope of business activities and the type of personal data processed.

In the following, we describe the basic elements of our DPMS in accordance with the auditing standard IDW PS 980 and considering IDW PH 9.860.1 (“Audit of the principles, procedures, and measures in accordance with the EU General Data Protection Regulation and the Federal Data Protection Act) as a non-exhaustive list.

In this context, the DPMS comprises all data protection-specific measures taken in the Group companies to comply with the applicable data protection laws within the material and geographical scope of “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC General Data Protection Regulation” (GDPR).

Our data protection organization is integrated as part of a holistic Governance, Risk & Compliance (GRC) System.

02

DATA PROTECTION CIRCLE

Customers, business partners and employees have a legitimate expectation that the data entrusted to us will be processed confidentially and only for the intended purposes. This DPMS applies to Ströer SE & Co. KGaA and all affiliated majority shareholdings that are subject to the territorial scope of the GDPR. Its purpose is to implement the principles derived from the GDPR as defined in Ströer's data protection policy and set out in line with the data protection circle:

2.1 Culture

Ströer is committed to the fundamental right to data protection. This right protects individuals from intrusion into their private sphere through the unnecessary, arbitrary, or disproportionate use of personal data. Safeguarding this right is part of the way we see ourselves as a company.

In an increasingly digitalized and data-driven economy, new technologies for data processing naturally also lead to larger volumes of personal data and their more diverse use. This makes it possible for Ströer to become more customer-oriented, innovative, agile, and comprehensively digital in its internal processes and its activities vis-à-vis stakeholders. At the same time, this is accompanied by the challenge of protecting the privacy of those affected in an appropriate manner.

The Ströer Group therefore has a central interest in ensuring that innovative technologies and new business models comply with applicable data protection regulations. With increasing digitalization, we therefore consider it important that Ströer also explicitly acknowledges its data responsibility within the scope of its business activities. Responsible handling of data in the interests of our customers, employees and other stakeholders will therefore remain one of our goals in the future and further strengthen trust in Ströer. The definition of the data protection strategy for dealing with data protection requirements helps us to achieve these goals in line with the specific activities of the group companies.

A good relationship with all stakeholders (employees, customers, business partners, suppliers, shareholders, etc.) is fundamental to this. Any violation of data protection laws risks permanently damaging our reputation and can lead to considerable damage and serious consequences for the Ströer Group. Furthermore, such violations, as well as for the employees involved, may lead to civil or criminal sanctions.

At Ströer, acting ethically and legally correctly is a core principle that is already expressed in the "Code of Conduct" and this includes compliance with data protection law. This is supported by the fundamental understanding at Ströer that compliance with applicable laws always takes precedence over business objectives in the event of conflict.

"We are aware of our obligation to respect the personal dignity, privacy and personal rights of all employees as well as our customers and business partners."

Stephan Schnitzler
Head of Governance, Risk & Compliance

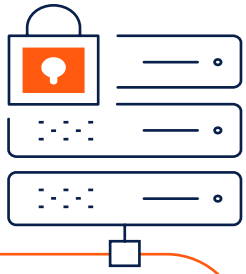
In addition, Ströer's "General Data Protection Policy" is based on the fundamental understanding that any processing of personal data must be carried out in accordance with applicable data protection laws, in particular the GDPR.

Our data protection culture is illustrated by the following declaration of the Group Management Board:

"In an increasingly digitalized world, data protection is a critical factor and the protection of personal data remains a priority in Ströer's compliance strategy. It is the responsibility of all of us to ensure compliance with the GDPR."

Henning Gieseke
Management Board

DATA PROTECTION IS PARTICULARLY IMPORTANT TO STRÖER FOR THREE REASONS:



FUTURE

The use of data is essential for many areas of our activities. Here we want to accompany further developments positively and continue to make positive use of the opportunities that arise from a growing supply of data. This is only possible if we also protect “data“ appropriately.

TRUST

Both our customers, users, our partners, and of course our employees, must be able to trust that their data and, where applicable, the data of their customers, users and partners is safe with us in order to share it with us and work with us.

COMPLIANCE

Corporate and personal success can only be achieved and secured in an environment of legal compliance. For us, compliance with legal requirements is a non-negotiable basic prerequisite for our activities. The basis for this is our “Code of Conduct“.

2.2 Targets

The legal obligations arising from the respective data protection regulations – in particular from the General Data Protection Regulation and the Federal Data Protection Act ("Bundesdatenschutzgesetz") – place complex and strict requirements on those who process personal data. Our aim is to ensure that all data protection requirements are complied with throughout the Group.

Everyone at Ströer is responsible for treating personal data with appropriate confidentiality and protecting it from misuse so that no one's right to privacy is impaired by the handling of this data.

All employees at Ströer will handle personal data of our customers, business partners and their colleagues with care and confidentiality and will comply with applicable law.

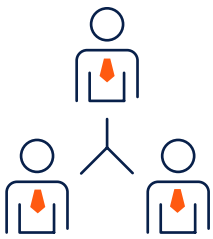
Everyone in the Ströer Group who is responsible for an activity involving personal data organizes the processing (collection, use, storage, deletion, etc.) of personal data in such a way as to ensure compliance with applicable law.

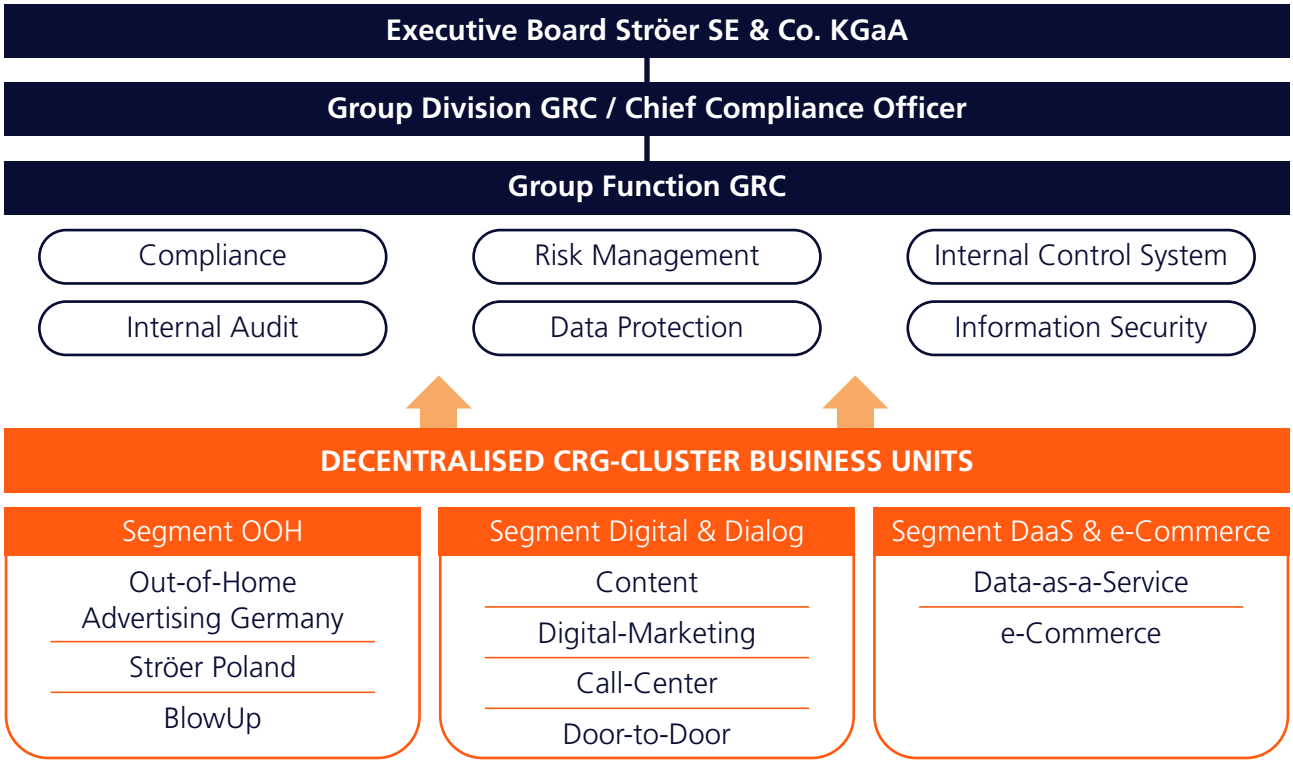
We also transfer these expectations to our suppliers and business partners through our "Code of Conduct for Suppliers and Business Partners".

THE DUTIES AFFECT EVERYONE AT STRÖER!

2.3 Organization

The Ströer Group consists of Ströer SE & Co. KGaA as the parent company and numerous subsidiaries. These group companies are divided into "clusters" in the Governance, Risk & Compliance organization.



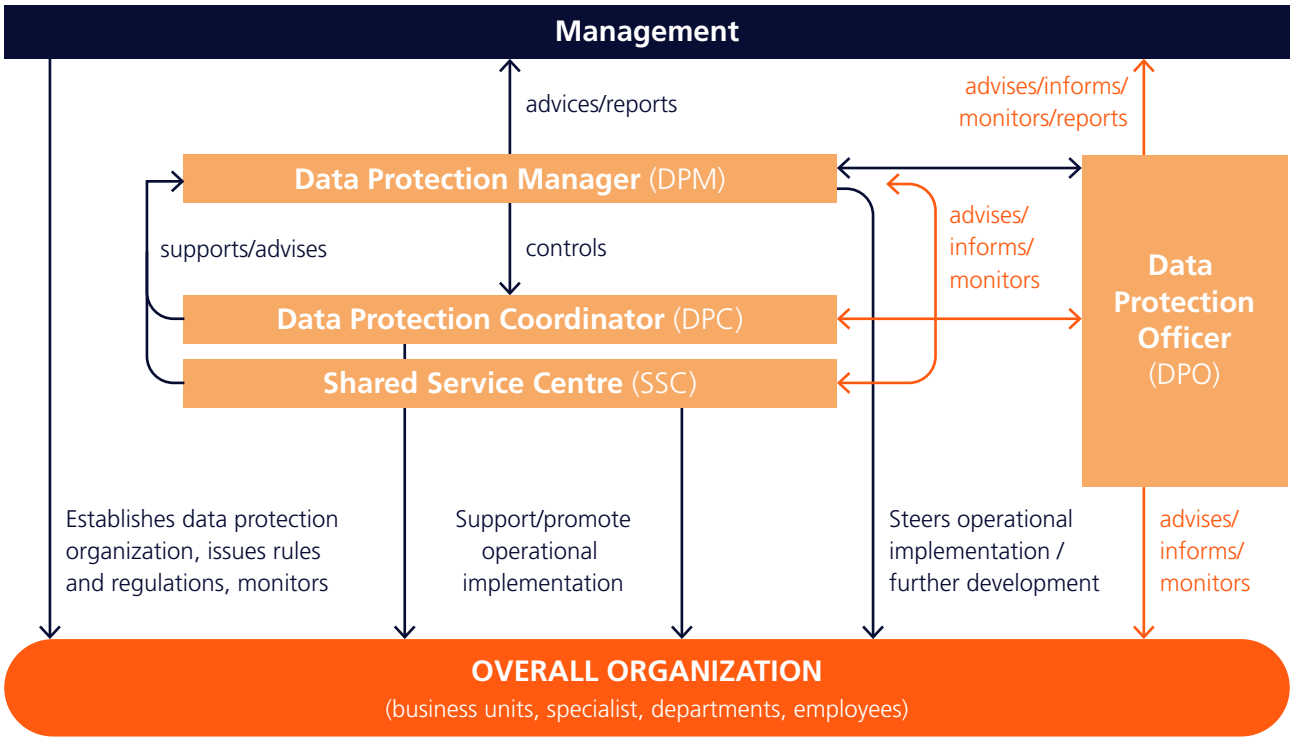


Within the decentralized clusters, compliance with data protection requirements must be ensured with regard to each individual processing of personal data ("processing activity"), at company level.

The Board of Management bears overall responsibility for compliance with applicable laws and internal standards. Ströer has established an interdisciplinary "GRC Committee" chaired by the CFO of Ströer SE & Co. KGaA, which is responsible for resourcing and for managing and monitoring the data protection organization.

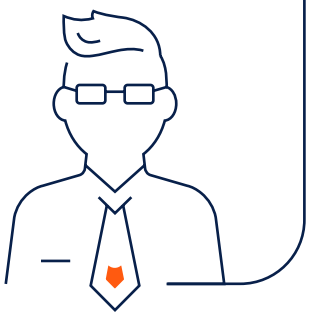
To the extent provided by law, each Group company appoints an expert Data Protection Officer (DPO) to perform the tasks defined in the GDPR, especially his function as contact person for data subjects.

A Data Protection Manager (DPM) is also appointed for each cluster. The DPM is responsible for compliance with data protection requirements over and above the statutory duties of a DPO. The management delegates to the DPM the performance of its duties under data protection law. The DPM is supported by Data Protection Coordinators (DPC) in the implementation of his or her tasks and can instruct them as necessary.



Operational data protection (such as ensuring the lawfulness of data processing operations; managing processors; ensuring compliance with internal data protection management processes, monitoring, creating appropriate documentation to demonstrate compliance with the GDPR, etc.) is the responsibility of the "Process Owner", "Product Owner" and "Contract Owner". They have sufficient knowledge and the necessary resources to perform their tasks, as well as the authority to modify or suspend data processing operations.

The Group IT and the Group Information Security Office (GISO) support defining technical and organizational measures in accordance with the GDPR and other relevant jurisdictions and implementing processes to ensure that the principles of "privacy by design" and "privacy by default" are considered when introducing or modifying a processing of personal data.

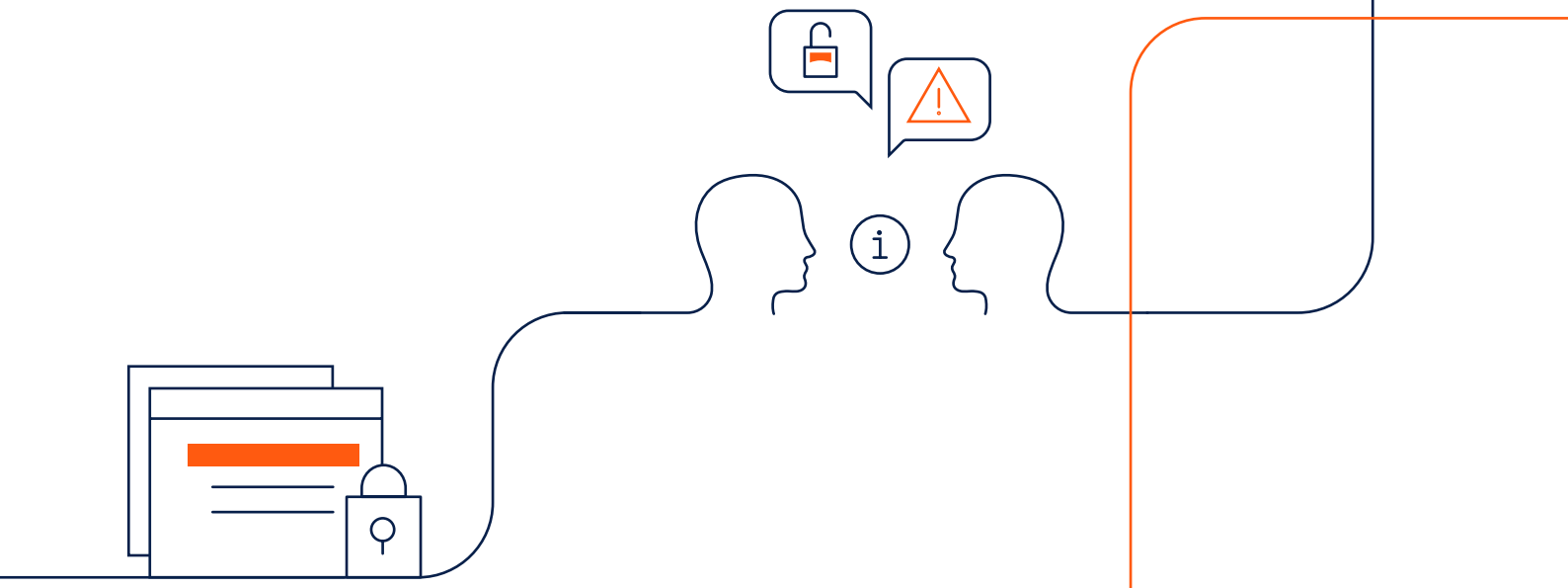


2.4 Risks

As part of an integrated corporate governance approach, the Ströer Group operates a comprehensive group-wide risk management system. The main data protection risks are also recorded and managed within this system.

Data protection risks are assessed both from the perspective of the natural person affected by the data processing ("data subject") and from the perspective of the company. The assessment of the risk essentially results from the category of data processed and the means used, the risk potential and the complexity of the processing.

The risk of each processing operation is assessed according to a specific methodology which considers both the types of data processed and the specific nature of the processing operation. This makes it possible to determine whether the processing of personal data poses a risk simply by virtue of the fact that personal data is processed at all, whether special categories of personal data are processed, or whether specific categories of data and risk factors indicate an increased risk of a processing activity in the data processing.



2.5 Program

The DPMS is based on globally binding corporate principles and supplementary guidelines. The core of the DPMS are the "Corporate Privacy Principles" (CPP). The aim of these CPP is to create minimum organizational standards and a uniform framework for the processing and protection of personal data in the Group and to prevent damage to Ströer. The CPP may be supplemented by additional guidelines applicable to specific countries or business units to comprehensively ensure compliance with statutory data protection requirements. The data protection program includes in particular:

- Notification and reporting of data breaches
- Records of processing activities
- Technical and organizational security measures
- Deletion/retention schedules
- Rights of the data subject
- Processing by processors
- Transfers to third countries

For example, the "Incident Response Plan" provides a framework for the effective identification, internal management, and external notification of data breaches. Data breaches identified during an investigation, general monitoring processes or otherwise must be promptly reported to the relevant DPM as required by the Policy and in the form specified therein. The DPO shall advise the controller on the need to notify the data protection authorities and/or the data subjects of the data breach and, where appropriate, issue the notification.

Our "General Data Protection Policy" requires each company in the Group to maintain records of processing activities and to implement a process to reflect changes and ensure the accuracy and completeness. We use market-leading data protection management software to manage such data protection-related tasks. For each individual processing activity, it must also be ensured that the processing is carried out in compliance with all applicable regulations. So-called "Process Owners" ensure lawful processing, i.e. they ensure that either an applicable legal provision or the demonstrable consent of the data subject permits the use of personal data and that all other principles of lawful data processing are complied with at all times.

This includes ensuring the implementation of appropriate technical and organizational security measures to protect personal data, including protection against unauthorized, unlawful processing or alteration of purpose and against accidental loss, destruction or damage, as well as measures for proper and timely erasure, taking into account the state of the art and the nature, scope, context and purposes of the processing, and the risk of varying likelihood and severity to the rights and freedoms of data subjects.

In addition, "Process Owners" shall provide data subjects with transparent information ("data protection notices") on data processing, enabling them to effectively exercise their data subject rights granted by law.

The introduction and replacement of processors are reported to the DPC by the "Contract Owners". The processors are regularly checked for their reliability to provide services for compliance with appropriate technical and organizational security measures; the control is carried out e.g. by interviews, document reviews, on-site investigations or other appropriate measures. The DPM maintains an overview of all processors commissioned by the respective company in its cluster.

Where a processing operation involves transfers of data to a third country, data controllers shall notify such transfers and appropriate safeguards and guarantees of third party rights, their enforceability and effective remedies shall be regularly reviewed.

As a Group, Ströer relies on internal international data transfers to make the data available to the relevant processors. To this end, we have defined

requirements for data transfers within the Group. Standard contractual clauses are in place between the relevant subsidiaries, for example, which provide for appropriate safeguards, enforceable data subject rights and effective remedies for data subjects.

2.6 Communication

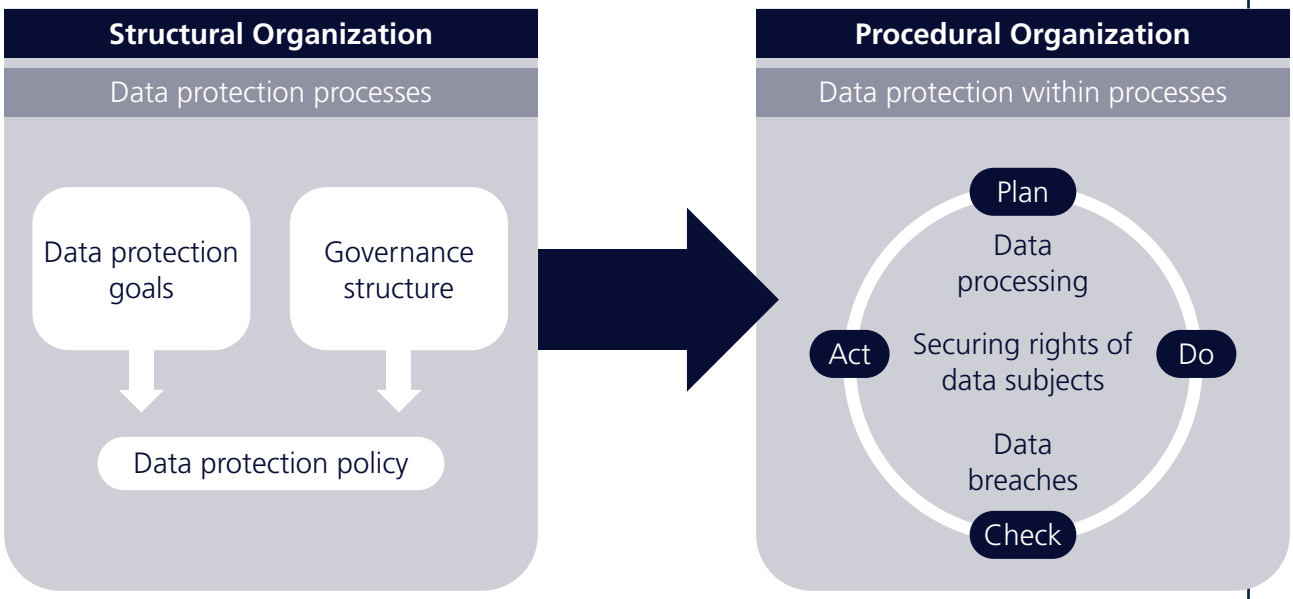
Communication and awareness-raising on data protection is broadly based and ranges from general information in the intranet "Ströernetz", in newsletters or other community channels that are accessible to all employees or addressed to specific departments, to target-oriented detailed information in the "Datenschutzkoffer", a data protection toolbox aimed at individual interest groups, to discussions among data protection stakeholders. Every year, Ströer also reports on its progress in data protection as part of the Group's sustainability report.

Data protection processes and standards are communicated to our employees at several levels. Training and awareness-raising measures are tailored to the risk profile of the business fields and the specific activities of the addressees. This includes basic training on the GDPR as eLearning, which is mandatory for all employees in the Ströer Group. In addition, voluntary eLearning sessions are offered, for example personal training sessions for "decision-makers" in data protection, as well as instruction for new employees as part of the onboarding process. The understanding that data protection is everyone's responsibility has also been strengthened by the Data Protection Confidentiality Agreement, which all employees are informed about before they start work. All employees can seek appropriate advice on data protection issues. Internally, they are free to contact the relevant Data Protection Manager, Data Protection Officer or Data Protection Coordinator in the data protection organization at any time.

The further development of the data protection training concept, in particular with regard to training for data protection stakeholders and other internal employees based on a risk-based approach (e.g. HR, Group IT and Marketing in connection with customer data), is firmly planned in the DPMS.

2.7 Monitoring and improvement

The ongoing development of our concepts, content, and tools to ensure adequate data protection has further improved the effectiveness of the existing DPMS.



The DPMS supports Ströer in planning, implementing and regularly reviewing data protection compliance measures in a structured manner. The data protection stakeholders working in the data protection organization analyze and use the results of the audits to continuously reduce data protection risks.

The data protection measures are also reviewed for effectiveness by internal controls and internal audit investigations. The data protection organization works closely with the internal audit department, which prepares and carries out internal audits in the Ströer Group on the basis of an audit plan derived from a risk-based audit approach.

Legal data protection matters are discussed and coordinated with internal and external legal advisors, and advice is provided on further improvements and new regulatory requirements.

The data protection organization is actively networked in external forums, which enables knowledge to be shared and processes to be benchmarked with peers. Best practices are identified, implemented and lead to improvements in data protection processes at Ströer. Identifying control deficits and implementing appropriate measures is part of Ströer's data protection reporting, including the development of key compliance activities implemented across several companies in the Group.

.

Ströer SE & Co. KGaA
Ströer-Allee 1
50999 Köln

CONTACT

Stephan Schnitzler
Governance, Risk & Compliance

Stephan Kuchenbuch
Group Data Protection

Published in November 2022