

International Comparative Legal Guides



Practical cross-border insights into data protection law

Data Protection 2023

10th Edition

Contributing Editors:

Tim Hickman & Dr. Detlev Gabel
White & Case LLP

[ICLG.com](https://www.iclg.com)

Expert Analysis Chapters

- 1** **The Rapid Evolution of Data Protection Laws**
Tim Hickman & Dr. Detlev Gabel, White & Case LLP
- 9** **Personal Data Breach Prevention and Response Strategy**
Daniela Fábíán Masoch, FABIAN PRIVACY LEGAL GmbH
- 15** **Initiatives to Boost AI and Metaverse Business in Japan**
Takashi Nakazaki, Anderson Mōri & Tomotsune
- 23** **“Selling” or “Sharing” Personal Information Under US Privacy Laws**
Paul Lanois, Fieldfisher

Q&A Chapters

- 27** **Argentina**
Marval O’Farrell Mairal: Diego Fernández
- 37** **Brazil**
Prado Vidigal Advogados: Pedro Nachbar Sanches & Gabriela Agostineto Giacon
- 46** **Canada**
Baker McKenzie: Theo Ling & Conrad Flaczyk
- 59** **China**
King & Wood Mallesons: Susan Ning & Han Wu
- 74** **Cyprus**
Harris Kyriakides: Michael Kyriakides, Eleni Neoptolemou & Munevver Kasif
- 86** **Denmark**
Lund Elmer Sandager Law Firm LLP: Torsten Hylleberg
- 97** **France**
White & Case LLP: Clara Hainsdorf & Bertrand Liard
- 107** **Germany**
Noerr Partnerschaftsgesellschaft mbB: Daniel Ruecker, Julian Monschke, Pascal Schumacher & Korbinian Hartl
- 117** **Greece**
Nikolinakos & Partners Law Firm: Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou & Alexis N. Spyropoulos
- 130** **India**
LexOrbis: Manisha Singh & Swati Mittal
- 142** **Indonesia**
ATD Law in association with Mori Hamada & Matsumoto: Abadi Abi Tisnadisastra & Prayoga Mokoginta
- 152** **Ireland**
ByrneWallace LLP: Victor Timon, Zelda Deasy, Seán O’Donnell & Julia Drennan
- 165** **Isle of Man**
DQ Advocates Limited: Kathryn Sharman & Sinead O’Connor
- 175** **Israel**
Naschitz, Brandes, Amir & Co., Advocates: Dalit Ben-Israel & Dana Zigman Behrend
- 192** **Italy**
FTCC Studio Legale Associato: Pierluigi Cottafavi & Santina Parrello
- 203** **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi & Masaki Yukawa
- 216** **Korea**
Bae, Kim & Lee LLC: Kwang Hyun Ryoo, Taeuk Kang, Minwoon Yang & Doyeup Kim
- 227** **Mexico**
OLIVARES: Abraham Diaz Arceo, Gustavo Alcocer & Carla Huitron
- 236** **New Zealand**
Webb Henderson: Jordan Cox & Ken Ng
- 247** **Nigeria**
Udo Udoma & Belo-Osagie: Jumoke Lambo, Chisom Okolie & Chidinma Chukwuma
- 261** **Norway**
Wikborg Rein Advokatfirma AS: Gry Hvidsten, Emily M. Weitzenboeck & Wegard Kyoo Bergli
- 274** **Pakistan**
S. U. Khan Associates Corporate & Legal Consultants: Saifullah Khan & Saeed Hasan Khan
- 283** **Peru**
Iriarte & Asociados: Erick Iriarte Ahón & Fátima Toche Vega
- 292** **Saudi Arabia**
Hammad & Al-Mehdar Law Firm: Suhaib Hammad

Q&A Chapters Continued

301**Singapore**

Drew & Napier LLC: Lim Chong Kin & Anastasia Su-Anne Chen

317**Sweden**

Synch Advokat AB: Karolina Pekkari & Josefin Riklund

328**Taiwan**

Lee and Li, Attorneys at Law: Ken-Ying Tseng & Sam Huang

338**Turkey/Türkiye**

SEOR Law Firm: Okan Or & Eren Kutadgu

348**United Arab Emirates**

Bizilance Legal Consultants: Saifullah Khan & Saeed Hasan Khan

359**United Kingdom**

White & Case LLP: Tim Hickman & Joe Devine

371**USA**

White & Case LLP: F. Paul Pittman, Abdul Hafiz & Andrew Hamm

Personal Data Breach Prevention and Response Strategy

FABIAN PRIVACY LEGAL GmbH



Daniela Fábíán Masoch

1 Introduction

Laws around the world impose strict data security obligations on organisations that process personal data, and in some cases require them to report data breaches to data protection authorities and individuals affected by the data breach. In addition to significant sanctions for failing to take appropriate technical and organisational measures (TOMs) to protect data, and potentially for failing to report a data breach as required by law, organisations may suffer, among other things: loss of stakeholder trust; reputational damage; and disruption of business activities as a result of a data breach, leading to economic losses. In addition, there are significant costs associated with managing a data breach and remediating the damage caused by the breach.

Investing in data security to prevent data breaches, such as those caused by cyberattacks or employee errors, and being prepared to respond in the event of a data breach is therefore worthwhile not only to comply with the legal obligations, but also to avoid negative consequences for the organisation and its stakeholders.

This chapter elaborates on what constitutes a personal data breach and what a data breach prevention and response strategy might look like. It is limited to dealing with data breaches involving personal data. It takes the requirements of the General Data Protection Regulation (GDPR) as a starting point, but without limiting itself to the GDPR. In particular, it considers the incident notification requirements under the new EU Directive on measures for a high common level of cybersecurity across the Union (NIS2), effective as of 16 January 2023, which significantly expands the categories of entities within the scope, including entities such as manufacturers of chemicals and medical devices, food processors, social network providers, and postal and courier services. With such an extension, a wide range of entities that did not fall under the former NIS Directive, will be subject to additional incident notifications. The NIS2 Directive must be transposed by the EU Member States into national law by 18 October 2024.

2 What is a Personal Data Breach and its Potential Consequences?

A personal data breach (data breach) occurs when personal data held by an organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. The GDPR defines the term “personal data breach” as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Privacy laws in other jurisdictions contain similar, though not identical, definitions. An “incident,” on the other hand, is defined by NIS2 as an event compromising the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or of the services

offered by, or accessible via, network or information systems. We refer to a potential data breach when personal data is affected.

The EDPB’s Guidelines 9/2022 on Data Breach Notification under the GDPR, adopted on 28 March 2023 (previously the Working Party Opinion 03/2014 (WP29) on Data Breach Notification), divide data breaches into three security principles:

- **Confidentiality breach** – where there is an unauthorised or accidental disclosure of, or access to, personal data.
- **Integrity breach** – where there is an unauthorised or accidental alteration of personal data.
- **Availability breach** – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Examples of data breaches include: the loss or theft of a data carrier (e.g., notebook, phone, USB stick, paper files) containing unencrypted personal data of customers or employees (breach in confidentiality, and potentially availability if there is no backup for the stolen device); the successful penetration of an organisation’s computer systems containing personal data for the purpose of copying, exfiltrating, and misusing personal data for malicious purposes (breach in confidentiality and possibly integrity); a ransomware attack in which the attacker encrypts data with a malicious code and then demands a ransom from the attacked organisation in exchange for the decryption key (availability breach, and possibly confidentiality breach); the unauthorised downloading of personal data by a terminated employee for further private use (confidentiality breach); and the inadvertent disclosure of personal data by an employee to unauthorised persons inside or outside the organisation, e.g., by sending it to an incorrect address or by sending a file that inadvertently contains personal data not intended for the recipients (confidentiality breach).

A data breach may have various negative effects on individuals and result in physical, material and immaterial damage. It may, for example, cause the affected individual to lose control over their personal data, to be restricted in the exercise of their personal rights, to suffer financial loss or personal disadvantage, emotional distress, embarrassment or humiliation, or to suffer damage to their reputation. Possible consequences may also include identity theft or fraud, loss of employment or business opportunities, unwanted marketing or spam, reversal of pseudonymisation, or other significant economic or social disadvantages.

Organisations can also suffer harm as a result of a data breach. Responding to a data breach and potential subsequent complaints and implementing remedial actions may have financial, legal and resource implications. Data breaches can further result in reputational damage and loss of stakeholder trust.

According to the Ponemon Institute’s 2022 Cost of a Data Breach Report, the average cost of a data breach was \$4.35 million in 2022. The average cost has increased by 12.7% from \$3.86 million in 2020, with costs being significantly lower for organisations with more mature security levels. The average total cost per record containing personal data was \$164. The longer it took

to detect the breach, the more expensive it was, with most of the costs related to detection and escalation, followed by cost of lost business (including business interruption and lost revenue due to system downtime, cost of lost customers and acquiring new customers, loss of reputation, and diminished goodwill). The remaining cost drivers were post-breach response, and notification. The costliest initial attack vectors were phishing followed by compromised business emails, vulnerability in third-party software, and stolen or compromised credentials.

3 Data Breach Notification Requirements

Many countries around the world have introduced data breach notification regulations. The first laws were enacted in the U.S. at the state level starting in 2002 (California). Other countries have followed, such as the EU Member States and the United Kingdom with the GDPR and the UK Data Protection Regulation (UK GDPR), respectively, as well as other countries around the world, such as Australia, Brazil, China, Colombia, Egypt, Ghana, Israel, Kenya, Mexico, New Zealand, the Philippines, Singapore, South Korea, Switzerland, Taiwan, Thailand and Uruguay.

Independent of data breach notification requirements, most countries in the world have introduced data security obligations that must be implemented by the affected entities, including data controllers and data processors. Such new legislation includes the NIS2 Directive and similar national laws, such as the UK's Network and Information Systems Regulations 2018 (NIS Regulations) and Switzerland's Information Security Act, as well as new EU laws related to the NIS2 Directive, such as the Critical Entities Resilience Directive (CER Directive), the EU Digital Operational Resilience Act (DORA) and the Cyber Resilience Act as part of the EU's new digital legislative package, addressing the cyber resilience of entities across the EU.

NIS2 significantly expands the categories of entities falling under its scope and applies to companies active in sectors including energy, transport, banking, financial markets, health, drinking water, waste water, digital infrastructure, ICT service management, public administration and space (essential sectors), as well as postal and courier services, waste management, manufacture, production and distribution of chemicals, production, processing and distribution of food, manufacturing, digital providers and research (important sectors).

According to NIS2 rules, essential and important entities are required to notify their computer security incident response team (CSIRT) or, where applicable, the competent EU Member State authority of any significant incident in a multiple-stage reporting system:

1. an early warning without undue delay and in any event within 24 hours of becoming aware of the significant incident, which, where applicable, indicates whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
2. an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident, which, where applicable, should update the information provided with the early warning and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise; and
3. a final report not later than one month after the submission of the incident notification, including a detailed description of the incident, specifying its severity and impact, the type of threat or root cause that is likely to have triggered the incident, applied and ongoing mitigation measures, and, where applicable, the cross-border impact of the incident.

The incident is significant if: (a) it has caused, or is capable of causing, severe operational disruption of the services or

financial loss for the entity concerned; or (b) it has affected, or is capable of affecting, other natural or legal persons by causing considerable material or non-material damage.

NIS2 sets out cooperation rules for the NIS2 competent authorities and the data protection authorities, and states that in cases where an incident to be reported under NIS2 also qualifies as a notifiable data breach under the GDPR, the NIS2 competent authorities should work in close cooperation with data protection authorities under the GDPR when addressing incidents resulting in data breaches. The NIS2 competent authorities must, without undue delay, inform the data protection authorities. However, where the data protection authority competent under the GDPR is established in another Member State than the NIS2 competent authority, the NIS2 competent authority must inform the data protection authority established in its own Member State of the data breach.

Depending on how the NIS2 Directive is implemented in the EU Member States, it may be required for organisations covered by the NIS2 Directive to report an incident under NIS2 that also constitutes a data breach under the GDPR to the NIS2 competent authority and the data protection authorities in the EU Member States concerned (or the lead authority, if applicable).

The notification obligation will continue to be a challenge for companies established outside the EU. While the Art. 29 Working Party recommended in its guidelines on notification of data breaches under the GDPR, last revised 6 February 2018, that notification should be made to the data protection authority of the Member State where the controller's representative in the EU is established, the EDPB now overturns this position in its Guidelines 9/2022 on personal data breach notification under GDPR, adopted on 28 March 2023, by clarifying that the mere presence of a representative in a Member State does not trigger the one-stop-shop system. Therefore, controllers established outside the EU without a main establishment in the EU must notify cross-border data breaches to any data protection authority in the Member States where the data subjects are located.

4 Data Breach Prevention and Response Strategy

Although security requirements and the conditions and modalities of notification obligations may vary from country to country, any organisation that processes personal data and is subject to security and notification obligations should define and implement a data security and breach management strategy to ensure adequate data security and risk mitigation in the event of an incident and be prepared to deal with any data breaches.

The data breach response strategy does not need to be stand-alone but can and should be aligned with other internal data-management and security strategies, e.g., information security, where possible. It should cover three key factors: prevention; response; and improvement.



4.1 Prevention – Implement appropriate TOMs

Even with the best possible security, data breaches cannot be completely avoided. However, data breaches are often the result of a vulnerable and outdated security regime or system weaknesses. Prevention through the adoption of appropriate security measures is therefore key to preventing vulnerabilities in systems or insufficient security that can potentially lead to a data breach.

Data and risk mapping: Only if organisations know what types of data breaches could occur and understand the characteristics of these breaches, can they take the necessary TOMs to reduce the risk of a successful attack or breach.

The basic prerequisite is first that companies know what types of data and personal data they process, who the data subjects are and their locations, where the data is stored and who should have access to it. This knowledge requires the mapping of all data systems, products and services that process personal data and their classification. Organisations should then assess the risk level to their organisation and to individuals in the case of a data breach, as well as identifying the possible types of attacks and based on that understanding and the level of risk, take the appropriate TOMs to mitigate the consequences in the case of a data breach.

Implementation of TOMs: Based on the risk level, such TOMs may include a state-of-the-art encryption of the data at rest and a separate back-up of the data to help mitigate the consequences of a successful ransomware attack, or the loss or theft of a device with personal data. In addition to a state-of-the-art encryption, measures such as key management, regular updates of systems, use of strong authentication methods like two-factor authentication, firewalls, etc. may help to mitigate the consequences of data exfiltration. Regular awareness campaigns and training to staff on security aspects, instructions on how to use company devices and information as well as the implementation of technical measures and controls may help to prevent human errors.

Applicable laws and competent authorities: Organisations should assess which data protection and other laws apply to them in case of an incident and data breach. This should include assessing whether an entity is covered by NIS2. Based on this knowledge, organisations should determine which authorities to notify in case of a NIS2 incident and data breach. This insight will help save valuable time in the event of an incident.

External resources and insurance coverage: Besides the implementation of robust TOMs, organisations should evaluate in advance what type of external expertise is required in the case of a data breach and ensure that such expertise is available on short notice, which may require the negotiation of frame contracts in advance. Additionally, organisations may consider holding an insurance policy for data breaches.

Data breach response plan: Finally, organisations should deploy a data breach response plan that sets out procedures, modalities, and responsibilities in the event the organisation experiences a data breach (or a suspected data breach, i.e., a security incident) to respond to a data breach in a timely and efficient manner.

4.2 Response – Implement a data breach response plan

4.2.1. Why a data breach response plan?

Due to the usually very short timelines for reporting a data breach to the data protection authorities and individuals (at least in some countries, including the EU), it is critical that each organisation handling personal data put in place a documented data breach response plan. Implementing such a plan can help

organisations in: (a) mitigating the impact on the organisation and affected individuals, and the costs resulting from the data breach; (b) meeting their data security obligations; (c) protecting important business assets, including personal data of their employees and clients and the company's reputation; (d) dealing with negative media or stakeholder attention; and (e) instilling public confidence and trust in the organisation's capacity to protect personal data entrusted to the company by properly responding to a data breach.

The data breach response plan should be aligned with other plans as appropriate, such as existing security incident response, disaster recovery, business continuity, or contingency plans. This approach can ensure effective management with clear responsibilities, avoid duplication, and leverage synergies.

4.2.2. Content of a data breach response plan

A data breach response plan should establish the rules and processes on how to handle a data breach in compliance with internal standards and legal and regulatory requirements. It should outline what a data breach is, possibly providing some concrete examples tailored to the specific organisation, allocate the roles and responsibilities for detecting, responding, and documenting a data breach, describe the process for handling a data breach, from detection to notification and risk mitigation, and specify the obligations towards third parties processing the data on their behalf.

4.2.3. Establishment of an incident response team

While in small organisations the managing director or owner is often the person who deals with a data breach, usually with external assistance, establishing an incident response team has proven effective in mid-sized and larger organisations. The purpose of such a team is to ensure that in the event of a data breach, the relevant functions are immediately engaged, and data breaches can be promptly addressed, the risks assessed, and any required notifications made in a timely manner.

The composition of the team will depend on the organisation and the nature of the business, but will typically require different skill sets, which can be ensured by involving internal functions and external legal, data forensics, and media management experts. Organisations should assess what type of external expertise will be needed in the event of a data breach in advance, and ensure that this expertise is available on short notice. The organisation should maintain and regularly update a current list of team members, including their roles, responsibilities, and contact details, as well as the contact information of their delegates. Team members should receive regular training including on compliance with the applicable laws and notification requirements and participate in mock exercises. The response team should consist of a core team that includes, at a minimum, the data protection officer and the information security officer, and should be extended to include other functions such as human resources, research and development, or communications, as well as outside legal counsel and forensic analysts, depending on the severity and nature of the incident.

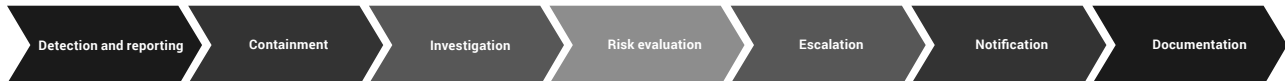
The incident response team should be responsible for managing the overall data breach, investigating, and reviewing the circumstances of the data breach and the facts of the case, engaging relevant functions and external experts, assessing the level of risk, determining remediation actions, determining the need for internal escalation, and notifying data protection authorities and individuals. The data breach response plan should identify the specific responsibilities of each member of the response team.

Furthermore, corporate management bodies should oversee, approve and be trained on the cybersecurity measures taken by the organisation, according to the new requirements of the NIS2 Directive.

4.2.4. Process for responding to a data breach

The process for responding to a data breach typically includes different steps, starting from the detection of the data breach and reporting to the immediate containment, investigation of the data breach, risk evaluation, internal escalation, notification, and documentation.

Detection and reporting: Each employee should understand how to recognise a potential data breach and know how to report such a data breach or suspected data breach (security incident) to the incident response team, who will immediately perform a preliminary evaluation and determine whether the incident qualifies as a data breach.



Containment: Once the source of the data breach has been identified, the data breach should be contained immediately to prevent further exposure of personal data, for example, and depending on the concrete impact, by remediating identified vulnerabilities in systems, recovering records, shutting down the compromised system, restricting access to data, recalling sent emails containing personal data that were inadvertently attached to the email or sent to the wrong recipients, or deleting them from the accounts of the unintended recipients.

Investigation: The incident response team should investigate and document the facts and circumstances of the data breach, including: the causes of the data breach such as any vulnerabilities in the computer systems; the nature of the data breach (breach of confidentiality, availability, or integrity); the nature, scope, and sensitivity of the personal data involved, as well as the origin of the data; the type, number, and location of data subjects; applicable data protection laws; and notification requirements.

Risk evaluation: Based on the outcome of the investigation and taking into account the type of personal data compromised, the extent of the data breach, and the type and number of individuals affected by the data breach, the incident response team must assess the level of risk of the data breach to the rights and freedoms of data subjects and the organisation. To assess the level of risk, they must determine the impact that the data breach could have on the rights and freedoms of individuals and the likelihood that this impact will actually occur. The greater the impact and the greater the likelihood, the higher the risk. Essential elements for determining the impact on individuals are the ease of their identification (how easily can an individual be identified from the compromised data?) and the severity (how much harm can be caused by the data breach?). Key elements in determining the likelihood of the identified impact actually occurring are the potential vulnerabilities due to the lack of appropriate TOMs and the ability to exploit those vulnerabilities or the intent of the individuals accessing or possessing the data (was the data exfiltrated by a hacker with malicious intent or sent by an employee to the wrong recipient in the same organisation by mistake?).

Escalation: The data breach response plan should define the internal escalation process, which should depend on the severity and extent of the breach, the level of risk identified, and the requirement for notification.

Notification: The incident response team determines, based on all the facts and the risk evaluation, whether the data breach must be notified to local data protection authorities and affected individuals, and if so, when, where, and how. At the same time,

the incident response team should address notification of other authorities, such as those responsible for NIS2 incidents, if the organisation is subject to NIS2 and it is a significant incident. The data breach response plan should identify which function is responsible for notifying the authorities and individuals. In general, the notification of a data breach is assigned to the data protection officer. Notification of an incident subject to other laws, such as NIS2, may be assigned to other functions. It is recommended that notifications be coordinated. It is also advantageous if scenarios requiring notification have already been worked through and documented.

Documentation: Any data breach, whether notified to data protection authorities and/or individuals or not, should be documented, including the facts and circumstances of the breach, its effects, and the corrective actions taken and planned to prevent future similar data breaches, the risk evaluation, and the appropriate justification for the decisions made with respect to the notification to data protection authorities and individuals.

4.2.5. Considerations in implementing a data breach response plan globally

Given the large number of countries with data breach notification requirements, globally operating companies are faced with the challenge of finding solutions that are as comprehensive and uniform as possible in order to, on the one hand, deal with data breaches uniformly and efficiently across the organisation and, on the other hand, take into account the specifics of the individual countries.

When implementing a data breach response plan globally, companies must take into account locally applicable data privacy and security laws, as well as notification requirements and modalities, languages, and cross-border data transfer restrictions, and align the data breach response plan accordingly. Companies should also decide what the internal reporting channel for discovered data breaches should be. Depending on their organisational set-up, they could establish one global reporting channel or separate regional or local reporting channels. Also, organisations must determine where data breaches should be documented (in a centralised system or locally), and whether a global incident response team should be deployed around the world, or regional/local response teams be established.

4.3 Improvement – Address security gaps to prevent future (similar) data breaches – regularly re-evaluate the data breach response plan to increase effectiveness

The third phase of the data breach response strategy consists of improvements in two respects: addressing identified vulnerabilities to prevent future similar data breaches; and increasing the effectiveness of the data breach response plan.

Address any identified security vulnerabilities to prevent future similar data breaches. Once the notification and documentation process is complete, the incident response team should determine and implement appropriate measures to prevent future similar data breaches. Depending on the concrete type of data breach and the root cause, such measures may include,

for example, conducting regular security audits and reviewing and updating policies and procedures in light of lessons learned, reviewing and amending contracts with third parties to ensure the appropriate handling of data breaches. Other measures may include, for example, restricting the downloading of personal data to mobile devices without adequate security protection, such as state-of-the-art encryption or the establishment of separate backups of specific data sets, and regular training for the business units concerned.

Periodically re-evaluate the data breach response plan to increase its effectiveness, taking into account changes in applicable data protection laws, best practices and internal business requirements.

5 Conclusion

Data security is one of the essential obligations of any organisation that processes personal data. A breach of the confidentiality, integrity or availability of data can have negative consequences not only for the individuals concerned, but also for the responsible organisation. A data breach can result in notification obligations, significant costs to contain the data breach and repair the damage caused by the breach, as well as loss of stakeholder trust, reputational damage, and business disruption. Investing in data security to prevent data breaches, such as those caused by cyberattacks or human error, and being prepared to respond in the event of a data breach, is therefore essential for any organisation to meet its legal obligations and avoid negative consequences for itself and the individuals affected.



Daniela Fábíán Masoch is the founder and executive director of FABIAN PRIVACY LEGAL GmbH. Daniela has more than 30 years of experience in privacy and data protection, employment law, risk and programme management, security, and related matters. She advises multinational companies, SMEs, and start-ups from various industries mainly in the EU, Switzerland and the US on data, data protection, security and related issues; particularly in the life sciences, pharma and medical device sectors.

Daniela supports her clients in evaluating, developing, implementing, and monitoring data protection strategies, governance models and global data protection programmes and data transfer mechanisms with a pragmatic approach. She also advises companies on data protection and cybersecurity, particularly on prevention, and the creation and implementation of data incident response plans.

Daniela is a member of various data protection associations and a lecturer at FernUni Switzerland for the CAS Data Protection and at Swiss Health Quality Association for Digital Marketing.

FABIAN PRIVACY LEGAL GmbH

Bäumleingasse 10
4051 Basel
Switzerland

Tel: +41 61 544 44 01
Email: daniela.fabian@privacylegal.ch
URL: www.privacylegal.ch

FABIAN PRIVACY LEGAL GmbH is a boutique law firm specialising in privacy and data protection laws and related issues, information security, data and privacy governance, risk management, programme implementation and legal compliance.

Our strengths are the combination of expert knowledge and practical in-house experience, a strong network with industry groups and privacy associations, and close cooperation with experts in data protection, cybersecurity, and cybercrime, and in jurisdictions around the world. We approach mandates with a global, solution-oriented, and practical approach, to deliver pragmatic and sustainable solutions.

www.privacylegal.ch



ICLG.com



Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms