SEP Hybrid **Backup** & Disaster **Recovery**

EU General Data Protection Regulation, EU NIS Directive & IT Security Act

A new, uniform data protection/security law for Europe.

By lawyer and IT law specialist Dr. Jens Bücking

Contents

*The author is a lawyer and IT law specialist. He is also a founding partner of the law firm e/s/b Rechtsanwälte (http://www.kanzlei.de), as well as a textbook author on IT law, a lecturer at the University of Applied Sciences in Stuttgart and associate professor at E.N.U. in Kerkrade, Netherlands.

** Disclaimer: This document constitutes a general legal assessment. It does not replace the legal advice given by a specialized lawyer. Please understand that despite the greatest possible care in its creation, there is no guarantee nor liability for its accuracy, timeliness or individual usability

Introduction

The EU General Data Protection Regulation (GDPR) has been in force since 05/25/2016 and becomes applicable law following a two-year transitional period. In the EU member states, the regulation replaces the previous 1995 EU Data Protection Directive and national data protection laws adopted along with it. As of 05/25/2018, it will be directly applicable to companies and authorities responsible for data processing (hereinafter: responsible parties).

In addition to the private sector, the GDPR will also fundamentally affect the public sphere. There are exceptions, such as court activities, public prosecution and police. However, the GDPR generally applies to all areas of federal, state and municipal law – albeit with numerous "flexibility clauses" allowing member states to introduce their own, specific provisions in the public sector that customize their regulations.

In order to ensure the full applicability of the GDPR, member states must partially adapt their national law. In Germany, this is first and foremost the task of the legislature. Self-governing bodies, however – above all municipalities and universities – are also called upon to adapt their statutes to the GDPR.

All data processing and related documents must be adapted by 05/25/2018.

The GDPR complements the EU NIS Directive and its model, the German IT Security Act of 2015, which – together with other European IT security legislation – form the future basis for a uniform data protection/security law for Europe. Its primary objectives are to secure public infrastructures, protect important assets and combat cybercrime. Damages from industrial espionage and cybercrime are highest in Germany, relative to the gross domestic product.

1. “Inescapable” (1) – the wide geographical scope of the EU GDPR

The GDPR will affect all companies doing business in the EU or in business relationships with EU-based companies and organizations, or collecting, processing and storing their data in EU member states. Therefore, the GDPR also extends to processors based outside of the EU.

Geographical implications primarily apply to IT within the EU, as well as to personal identifiable information (PII) processed by EU subsidiaries of responsible parties or their contractors, regardless of “where” – that is, whether or not the data processing itself takes place within the EU. Furthermore, it also applies to processing the PII of EU citizens by data controllers or processors outside the EU, as well as to data processing by data controllers outside the EU insofar as this concerns offers from online shops that seek to do business in the EU, regardless of whether their offers are chargeable or free. It also applies to goods or services offered to EU citizens (in which case an EU representative must be appointed), to profiling outside the EU whenever EU citizens are targeted, and finally – as a “catch-all” standard – to whenever the law of an EU member state applies to the data processing in question – which is virtually always.

The GDPR will therefore also have significant consequences for non-European companies active in the EU, as their primary point of contact is business activity in EU member states .

Since the GDPR does not constitute a dispositive right that could be contractually excluded by contracting parties for their data exchange, there is literally “no escape” from the regulation’s scope, which will also apply to the UK in the post-Brexit era.

2. “Inescapable” (2) – the extensive interpretation of the scope of “personal data” within the meaning of the EU GDPR

All organizations that collect, process and store PII are affected by the GDPR. By definition, PII is all information about a person, whether it relates to their personal or professional life. This includes, for example, names, photos, e-mail addresses, bank details, posts on social networking websites, medical data and IP addresses, even if these are dynamic. If responsible parties have “legal means” that allow them to identify the person behind an IP address, this already suffices. Whether allocation to an identifiable person actually occurs in a specific case is irrelevant, with the regulated matter only whether the legal means generally enable responsible parties to do so. Only in the case of absolutely non-traceable, anonymous (e.g. purely statistical or de-personalized by state-of-the-art encryption) data can the GDPR safely be overlooked. The solution required for permissible implementation and distribution of “Industry 4.0” (I4.0) and big data projects and products is therefore processes that reliably ensure absolute anonymization, so that no one – not even an external “super user” – is in a position to link processed information to a specific person. Only when personal referencing is “absolutely impossible to produce” is data anonymous in the legal sense, and outside the GDPR.

3. The most important reforms

Besides the maxims of "privacy by design" and "privacy by default" or the legal and control measure of the "Data Protection Impact Assessment" (DPIA), which are all yet to be explained in detail, substantial reforms of the conventional European data protection law include above all the rights to be forgotten, to data correction, cancellation, blocking and data portability and the obligation to notify of data protection breaches. Documentation requirements are being significantly expanded in terms of content and will be extended to include the processor as well in the future. The GDPR also visibly extends the applicability of EU data protection rules to processors and their clients in third-party countries. The ability for contract processors to be held liable for data breaches in their contract data processing is another addition, explained in detail below.

4. Order processing: new liability concepts for cloud & co.

Contract data processing is only permissible if permitted by law or if a written or electronic contract explicitly governs it. The processor must be carefully selected according to criteria such as reliability, performance and state-of-the-art technical and organizational security measures, and then checked before and regularly during the life of the contract data processing.

The corresponding contract must meet certain minimum content requirements. As before, processors may only process data when instructed by responsible parties. As a general rule, in cases where processors do not adhere to the limitations of the use of the data given to them, they then "mutate" into responsible parties – in a state of unlawful action. Original contractors must then be able to explain why and how processors were able to violate their instructions. Such cases assume joint legal responsibility (and liability). An important consequence of shared responsibility lies in the joint and several liability for all resulting damage:

In cases of doubt regarding breaches of the GDPR's provisions on contract data processing, liability is assumed with the part(y/ies) responsible for data processing. Under civil law, the responsible party and the processor are generally jointly and severally liable to any parties concerned. However, the liability of the processor is limited to duties specifically imposed on it (unless it has overridden the responsible party's instructions). Both the responsible party and the processor stand at risk of being fined.

In this context, it should be remembered: data center operation, ASP, SaaS, hosting and cloud are, without exception, all considered contract data processing constellations within the meaning of the GDPR.

According to new law, contract data processing can also take place outside the EU, whereby the GDPR is still applicable and remains the same. The regulation provides data controllers (i.e. all transfers of PII, especially in the case of contract data processing) certain legitimacy with "insecure third-party countries" where no adequate level of data protection can be established. These include, in particular, the assumption of binding and enforceable guarantees between government agencies, company-wide binding corporate rules (BCR) and (as before) standard data protection clauses if previously approved by the EU Commission. The possibility now exists within BCR not only for members of a specific group of companies but also for a group of companies pursuing a joint economic activity – as well as within a subcontractor relationship or a customer/supplier relationship – to create among themselves and mutually a legitimate basis for data exchange.

5. Data protection impact assessment

The GDPR also requires modern, effective data protection and security concepts as well as the new DPIA, which is previously unknown to data protection law, if the application or introduction of new IT procedures entails a high risk for the rights and freedoms of those affected. All existing and upcoming new projects in the field of IT must be checked (and documented accordingly) as to whether a DPIA is necessary.

Management must therefore create structures that ensure that DPIAs are comprehensively and properly executed and documented. Documentation is to be made in every case, even if it is determined that a DPIA will not be performed.

The legal uncertainty inherent in these assessments is mitigated by the fact that the GDPR requires data protection supervisory authorities to publish lists indicating in which cases a DPIA is necessary in case there is any doubt.

6. Data protection concept and technical-organizational data security measures

The provisions of the GDPR on data security are for the most part based on the domestic regulations of the German Federal Data Protection Act (BDSG). An appropriate privacy policy is a central pillar. Responsible parties must be able to ensure and prove that they comply with the GDPR by means of technical-organizational strategies and their implementation. This can be verified through certification or regulatory approval of BCR.

The technical and organizational measures for data security should in principle be based on a risk assessment. Similar to the subarea of corporate governance, known from stock corporation and commercial law with its legal obligations for efficient risk management (and an internal control system related to this), this risk assessment should be documented. The same applies to measures derived with regard to IT security and risks to the company as a result of data loss or breaches of data secrecy and business confidentiality.

Measures must take the state-of-the art in technology for specific sectors and data processing situations, as well as technological development into consideration. An early and regular target/actual analysis with risk assessment, with a corresponding data protection/security impact assessment, is therefore strongly recommended. This gap analysis is an important component in the implementation of the transparency, documentation, contract data processing and security management obligations postulated in the GDPR. In a first step of the gap analysis, all organizational units, processes and legal units affected by the implementation of the regulation should be identified.

7. Data protection through technology

The GDPR is based on the maxims of "privacy by design" and "privacy by default" (for example, forms and explanations, such as in the context of consent). The principle of data protection by technology requires that data protection must be "built-in" throughout the entire lifecycle of technology, from the earliest development phase through its introduction and use until final decommissioning. Identifying risks and resulting measures to mitigate them must thus be conceptually developed and documented in advance of the deployment of the technology. They must ensure a level of protection appropriate to the risks arising from processing and the nature of the data to be protected.

8. Notification obligations for infringements

In the future, any breach of data protection must always be reported to the supervisory authorities immediately, but no later than 72 hours after notice has been received. Cases are exempted in which responsible parties demonstrate there is no risk

for the rights and freedoms of those affected. If they want to avoid fines, they must establish a reliable process for reporting management – or essentially report any data breach. In any case, companies must document injuries and corresponding risk forecasts without exception (see RMS, ICS in accordance with the German Stock Corporation Act (AktG) and HGB, SoX, SEC, etc.).

Similar to the German model in Section 109a TKG, "data breach notifications" should be considered essential in the event of a security incident. Affected parties do not have to be notified if the supervisory authority is shown proof that suitable technical safety precautions have been taken. In the case of sufficient security measures and/or regular encryption of data or removal of risk, a report to the supervisory authority is not required. The GDPR thus grants privileges through IT security.

9. Operational and official data protection officer

The appointment of an operational data protection officer will be made in the future on a voluntary basis, unless the appointment is required by EU or national law. However, this is the case in most EU member states, but with different entry thresholds according to company size. Germany will retain its previous obligation to appoint an operational data protection officer. Public authorities that currently process personal data always have to appoint a data protection officer.

Another new measure is the obligation of a control/monitoring function for management instead of the previous (mere) duty to inform. The role of the operational data protection officer will therefore be strengthened by the GDPR in the future (although it will continue to be without authority to directly instruct). However, in addition to management, the CIO and compliance officers are now also confronted with a liability risk if they do not duly fulfill legal and other responsibilities.

10. Fines, damages, processing stoppages: stricter sanctions

With the GDPR's entry into force, companies, their management (and, if applicable, the supervisory bodies, in particular the Supervisory Board) and their special representatives for compliance, data protection and information security are threatened with significantly higher risks of liability than before.

The GDPR generally calls for sanctions to be effective, proportionate and dissuasive. It sets the level of fines and extends the imprisonment framework compared to the previous law. As a result, sanctions are usually equated with liability. In the case of the GDPR, liability implies the full range of civil and public sanctions. This includes, in particular, criminal penalties (fines, imprisonment), administrative penalties/fines and regulatory measures that may lead to the cessation of certain (business) activities and computer processes or even the closure of the business.

Liability may also extend to natural persons. If the fine is limited to the company itself, the control and supervisory body responsible will, of course, still be required to file recourse claims against the responsible parties.

In contrast, civil law claims are usually aimed at receiving compensation for damages. Claims arising from the violation of the GDPR also include pure financial losses (lost profits in particular). There is no maximum liability here. The calculation method for the fines that can be imposed for violations of the GDPR is global consolidated sales. Fines will be assessed in two stages (with the possibility of imprisonment in abusive cases): at level 1 for general infringements (e.g. of the regulations on contract data processing) up to EUR 10 million or 2% of global turnover, whichever is the higher amount, and at level 2 (violation of the principles of data processing, e.g. in the case of invalid consent, infringement of rights of the individuals affected, violations of provisions of international data transfer, regulations of member states such as in the area of employee data protection, non-compliance with instructions or conditions) up to EUR 20 million or 4% of global turnover, whichever is the higher amount. Until now, fines in Germany have only reached up to EUR 300,000 for material data protection violations and EUR 50,000 for formal violations. What is new is the penalty range of up to 3 years for cases in which the responsible party knowingly, without being authorized to do so, transmits or otherwise makes accessible personal data of a large number of people to a third party and is thereby commercially active.

11. Impact on Industry 4.0 and big data

The booming trends of Internet of Things (IoT) and I4.0 are, simply put, new, innovative business models made possible by rapid technical developments in the field of terminal connectivity, autonomous "machine decisions" by artificial intelligence (AI) systems and of big data readability through high-performance computing (HPC). The evaluation and control of such systems is carried out by data exchange, usually taking place across national borders.

Big data, I4.0 and AI processes must therefore be planned in advance in terms of international data protection law, particularly with the inclusion of the new data protection obligations on "privacy by design/default" and the data protection impact assessment. (This shall not apply, as mentioned, in the case of the resolution of direct personal reference. Since this requires the absolute anonymization in dealing with "everyone," effective and up-to-date encryption and documentation are needed.)

Data protection acts to which the GDPR applies collect, process and use personal data. Subcategories of this processing are storage, transmission, modification, blocking and deletion. "Using" is a catch-all for any other use. The entire data processing value chain is therefore subject to data protection laws, from generation/collection to deletion.

For the design of AI, big data and I4.0 processes, determining principles of EU data protection law should be taken into closer account, namely the general prohibition of processing personal data subject to authorization, the purpose limitation principle and the need for justification (law, consent), which in turn affects the intended use. This means that the use of any existing data for other purposes, or the merging of data with data from other sources, or any change of purpose requires new, additional justification.

This often leads to problems with these processes, since data has to be torn from its original purpose context, brought together, restructured and analyzed, then used in new ways. Individual consent does not seem feasible here in view of high efficacy hurdles. Consent would be effective only if it were declared on a sufficiently informed basis and complied with the provisions of the GTCT, in particular the requirement of transparency. Another shortcoming is the revocation of consent at any time.

As far as legal justification facts are available, they should be used primarily for I4.0 processes. Alternatively, it would require contract management to ensure that the respective data processing is needed to initiate and execute a contract with the individual(s) concerned, so that the appropriate design of the contractual relationship is the second means of choice. Only if and insofar as legal justifications do not intervene, should the instrument of consent be used.

12. IT security legislation in Europe

According to statistics, 70% of companies that experience data breaches have to cease operations within 18 months. In the field of industrial espionage, damages amount to EUR 51 billion per year in Germany alone, the largest attack and espionage target in the EU; globally, according to Europol, this figure is estimated at EUR 290 billion. Most cyberattacks are not even chiefly used to obtain specific information – the majority of cases are targeted at pure sabotage.

Particularly popular in recent cybercrime, are methods that spread malicious code over the Internet through websites and services of uninvolved third parties. According to the German Federal Office for Information Security's (BSI) situation report, these forms of distribution are among the most significant threats to network security: 75% of websites are classified as vulnerable. In the case of unwanted hosting of malware on websites, Germany ranks second worldwide.

It is estimated that damages from cybercrime in general amount to USD 400 billion worldwide. In terms of gross domestic product, Germany has been an unfortunate leader in attacks and damages in the field of IT for years.

The overwhelming number of security incidents never becomes public knowledge because affected companies' desire to protect their reputation. Therefore, reliable figures on individual damages due to internal IT breakdowns (faulty hardware /

software failures, staff/maintenance company failures, etc. without third party / external influences due to hacking, DoS or malware, for example) cannot be obtained. However, there are exceptions that are due to the prominence of the companies involved, as well as in the widespread involvement of the user community and the associated disclosure obligations.

12.1. Prominent disaster cases

One such sensation was the data disaster in the cloud service "Amazon EC 2" in April 2011, in which an unknown volume of data was irretrievably lost. Something similar happened in another cloud service in October 2009: a server error led to extensive data loss for users of the service "Sidekick," which T-Mobile offered together with the Microsoft subsidiary Danger. The Telekom Group was again criticized in the fall of 2010 for data loss in their e-mail center. According to reports, settings in the inbox folders filed with "Never delete" were overwritten with a default retention period of 90 days as a result of an update. Business e-mails older than 90 days were irretrievably lost, according to users. At the administrative level, state data protection authorities began to initiate fine proceedings in March 2016 against companies that – in the wake of the abolition of "Safe Harbor" as the legal basis for the data exchange with the US by a judgment of the ECJ on 10/06/2015 – continue to transfer personal data for data processing to the US.

12.2. EU NIS Directive

Additional specific IT security regulations that prescribe corresponding safeguards are distributed in various legal works and usually concern individual sections of the economy that are particularly worth protecting, or certain categories of data. The EU Directive on Information and Network Security from February 2013 (NIS Directive) should be mentioned here as a supranational example. In addition to the energy, banking, transport and health sectors ("operators of essential services"), Internet services, such as search engines, cloud providers and platform operators, are required to take action to improve their resistance to cyberattacks, to report major incidents to national authorities and to publish them under certain conditions.

12.3.Minimum requirements for IT security

Overall, important common technical and organizational standards, such as encryption, configuration error-free Internet and special security software (firewall, malware scanner, "intrusion detection" and "data loss prevention"), backup and information security management systems, data protection/security concepts to be continuously updated (including measures for attack prevention and disaster recovery / business continuity management), can be filtered out as state-of-the-art and best practice.

Given the sharp rise of cybercrime and the resulting billions in economic losses, particular importance is attached to appropriate emergency plans in which responses to attacks and disaster scenarios are to be defined and regular emergency simulations are to be conducted.

The technical and organizational precautions taken must be documented and assessed according to the latest conditions, so that, where appropriate, a knowledgeable third party can substantially review implemented measures and a court can reach an opinion as to responsibilities in the area subject to compulsory or ancillary contracts.

12.4. IT security jurisdiction

Jurisdiction also emphasizes that reliable IT security with regard to mission-critical data is one of the entrepreneurial preconditions in the age of digital data processing. The following statements are of particular relevance to a company's practice in domestic jurisdiction, where mostly liability cases in connection with the loss of an important or negligent breach of the confidentiality of confidential data are the cause of damages – as well as personal (manager liability) claims for damages:

- Jurisdiction regards the security of communication as a compliance-relevant obligation. Company-critical, – and especially

evidentiary, – documents must be stored for reasons of legal certainty and evidence. If this is not possible, a case could be lost under the mere burden of proof aspects due to "due diligence."

- Outsourcing of IT security alone is not enough to "exculpate" the delegating company and its management to the detriment of contracted IT companies (such as cloud providers or IT maintenance companies), i.e. from the liability responsibility for the protection and security of its data and systems. This may even apply to a fault of the external IT service provider in cases of data loss, if the contracting company has caused the consequences of this loss due to unreliable disaster and backup strategies. The proportion of contributory negligence can reach 100%, meaning full liability by the company for the resulting data loss and thus the resulting financial loss.
- Attention should also be paid in this context to the reversal of the burden of proof that, in cases where there is a dispute as to whether responsible members of management have used the diligence of a prudent and conscientious manager, they have the sole burden of proof for their exculpation.
- With respect to disaster management, jurisdiction requires as a general duty of care and due diligence that regular and reliable up-to-date, uninterrupted data protection routines are used in the area of the productive system, archive system and backup. External specialists – such as IT companies commissioned with maintenance and support or data center operators who work with company data by way of order data processing – may also take this as a matter of course without any special obligation to inquire. Conversely, however, in case of doubt, these commissioned third parties are obliged, even without explicit agreement, to take data protection measures, particularly backups, if their contractual obligations include the processing of company data.
- In addition, audit-proof archiving processes, firewalls, filtering and monitoring systems, encryption in any case for particularly sensitive data, as well as continuity management, which ensures a restart after restoration of the system and data in the event of damage, are counted among corporate IT protection obligations.
- In terms of the organization, appropriate IT company and privacy policies and employee training and education are required.
- The lack of an IT security concept consequently entitles a company to terminate the contract of employment concluded with a member of the Management Board extraordinarily and with immediate effect, or to consider a deficiency in the documentation of an early detection system with respect to the company as an important reason for contestability of the resolution on the discharge of liability of the entire Management Board.

Companies with effective business activities in the UK and the US are particularly exposed to the special significance (and considerable sanction consequences) of complete and evidential document management. Accordingly, civil procedure codes in the UK, for example, were supplemented in 2010 with regulations on electronic provision. The same applies to additions to US civil procedure law in 2006. As part of these developments, new sanctions for confidentiality and privacy violations were also implemented.

In summary, jurisdiction increasingly establishes general due diligence requirements for effective, up-to-date IT security against the backdrop of regulations that broadcast to other sectors of the economy (such as the Sarbanes-Oxley Act or the Basel Capital Accord). The tendency is on the rise for courts to request submission of data, even if it was stored long ago in large, possibly external or international (backup) storage and is therefore difficult to obtain, for an open court proceeding in a "proof" form. This obligation is independent of any force majeure. If necessary, this requires the use of state-of-the-art IT systems that provide strong evidence for evidential security and ultimately legal certainty.

Legal certainty through technical safety:

Solution concepts from SEP

SEP sesam secures business-critical information, applications, databases and systems that store all types of information, from sales and customer relationships, to production and management, to financial and business transactions. Due to this immense importance, a comprehensive business continuity strategy is needed that focuses on Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs), which are essential in a disaster recovery scenario.

The consistent SEP sesam Hybrid Backup and Bare Metal Recovery solution prevents data loss and can restore the entire environment after a disaster recovery scenario such as:

- force majeure
- hardware errors
- human failure
- data corruption
- logical and software errors

Even after an attack with an encryption Trojan, SEP backup data can be restored using the proven support of offline media.

SEP sesam's cross-platform Hybrid Backup and Disaster Recovery Solution is optimized for securing virtualized and physical environments and ensures compliance with legal requirements in heterogeneous IT environments. Encryption is a key technical element. SEP Encryption is performed with the cutting edge Si3 deduplication and replication technologies. Secure data retention is carried out by encryption of the SEP Si3 DedupStore. After decomposing the data stream into blocks and compressing each block, each individual block can be encrypted using an arbitrarily definable key. To restore the data, the key can be stored in the database of the backup server or the data owners must authorize a restore with their personal key. This encryption guarantees BSI compliance.

There are a number of technological approaches that help meet legal requirements.

Key elements of SEP sesam for legally compliant data security:

- Encryption of backups on backup media (Band, DataStore, Si3 DedupStore)
- Encryption of the data stream
- Encryption of communication
- External passwords for restoring according to the 4-eye principle
- Efficient disaster recovery for Windows and Linux
- Free of spyware
- Media discontinuity: support for offline and WORM media
- Manufacturer-corresponding backup and recovery
- Data can be backed up at various levels (for example at the hypervisor and application level)

- Cross-site data protection
- Automatic migration or copy of backup data to different backup media
- Full support of open source operating systems on the backup client and backup server side
- Legally secure backup of all company data
- Network security in firewall environments by restricting communication and data transport to a few dedicated ports
- Scheduled and automatic restore on stand-by systems to verify backups (can also be used for audits or documentation)
- Disaster recovery during operation, including reporting in physical environments (requires a test-target server) and in virtual environments

With SEP sesam, data is protected 24/7 and is always available. SEP's reliable backup solution is characterized by a large number of certifications for well-known application, system and hardware providers (e.g. SAP, Oracle, Novell, Red Hat, SUSE, Citrix, Microsoft, VMware, IBM, Fujitsu, Intel and more). These certifications ensure that original manufacturer support (e.g. SAP) is not lost. SEP's versatile and scalable data protection is ideally suited for medium to very large companies/ organizations and integrates seamlessly into any IT environment. It is important to point out that a technical solution is only one component of a complete compliant solution. The technical / software solution must be adopted to an organization's procedures, processes, concepts, risk analysis, documentation, etc. in order to obtain a holistic compliant solution.

The global solution - Made in Germany

Reliable restores, a flexible licensing model, German quality with high product standards and an attractive price-performance ratio are only four of countless arguments why organizations and enterprises trust in the Hybrid Backup solution SEP sesam. Even in heterogeneous IT-infrastructures, backups and recoveries are highly scalable, consistent and incredibly fast - especially in case of a disaster.

- Consistent backups and restores of all company data
- Flexible license models
- German quality and product standards
- Attractive price-performance ratio

Abbreviations:

- BCR: Binding Corporate Rules
- BSI: German Federal Office for Information Security
- DPIA: Data Protection Impact Assessment
- HPC: high-performance computing
- I4.0: Industry 4.0
- IoT: Internet of Things
- AI: artificial intelligence
- NIS Directive: EU Network and Information Systems Directive
- PII: personal identifiable information
- GDPR: EU General Data Protection Regulation
- BDSG: German Federal Data Protection Act

Headquarters (EMEA):
SEP AG
Konrad-Zuse-Strasse 5
83607 Holzkirchen, Germany
Phone: +49 8024 46331 0
Fax: +49 8024 46331 666
Email: info@sep.de

SEP USA:
470 Atlantic Avenue, 4th Floor
Boston, MA 02210, USA
Phone: (+1) 617-273-8200
Fax: (+1) 617-273-8001
Email: usa@sepsoftware.com

SEP APAC:
3 Spring Street
Sydney NSW 2000 n, Australia
Phone: +61 2 9659 9590
Fax: +61 430 196 446
Email: apac@sepsoftware.com