Datenschutz 2020

Wohin geht die Reise?

Forensische Spurensicherung: Fehler bei internen Untersuchungen können teuer werden

Dieser Artikel befasst sich mit häufigen Fehlern bei internen Untersuchungen. Ziel ist es, diese dem Leser aufzuzeigen, damit sie bei einer eigenen Untersuchung vermieden werden können. Der Autor arbeitet selbst seit 8 Jahren im Bereich der Computerforensik und Ediscovery und hat in diesen Jahren etliche „aufregende" Sicherungen von elektronischen Beweisen miterlebt – sogar bis zur Androhung von körperlicher Gewalt durch den Betriebsrat eines untersuchten Unternehmens.

Interne Untersuchungen & VerSanG

Die meisten Probleme und unerfreulichen Überraschungen lassen sich durch professionelle Planung, Durchführung und Knowhow vermeiden oder zumindest entschärfen. Gerade im Hinblick auf den neuen Referentenentwurf des Verbandssanktionsgesetzes wird die professionelle Durchführung von internen Untersuchungen immer wichtiger. Der vorgeschlagene Strafrahmen liegt, wie beim Kartellrecht, bei bis zu 10% des Jahresumsatzes eines Unternehmens. Eine Minderung ist durch frühzeitige und vollständige Kooperation mit den Behörden möglich. Es kann sich also finanziell erheblich lohnen, gut auf eine interne Untersuchung vorbereitet zu sein.
Die rechtliche Einschätzung soll jedoch nicht Teil dieses Beitrages sein, hierfür sind die Kollegen in Anwaltskanzleien zuständig.

Häufige Fehler bei internen Untersuchungen

1. Zu spät anfangen
Die Dauer einer Datensicherung ist nicht zu unterschätzen. Besonders bei Archivdaten können Wochen bis Monate vergehen, bis die Daten eines einzelnen Mitarbeiters kopiert sind. Dasselbe gilt bei ausgeprägter Homeoffice-Kultur oder mehreren Standorten. Hinzu kommt zusätzliche Zeit für Aufbereitung, Durchsuchung und Sichtung. Daher ist es für Unternehmen vorteilhaft, die Verfügbarkeit aller Datenquellen zu kennen. Die Unternehmens-IT und ein Computer-Forensik-Anbieter sollten frühzeitig involviert werden, um im Verdachtsfall schnell und umfassend reagieren zu können.

2. Unzureichend Daten sichern
Am Anfang einer Untersuchung weiß man selten genau, wann und bei wem ein Compliance-Verstoß vorliegt – bestenfalls gibt es Hinweise. Daher gilt zunächst: Sichern, sichern, sichern. Denn vielleicht werden bestimmte Verdächtige durch neue Erkenntnisse erst später in die Untersuchung einbezogen. Wichtige Indizien auf deren Geräten könnten dann bereits gelöscht worden sein.
Will man aufgrund mangelnder Beweislast einige Daten zunächst nicht in die Untersuchung mit einbeziehen, können diese – verschlüsselt und in Beweismitteltüten eingeschweißt – an einem sicheren Ort im Unternehmen verwahrt werden. Speicherplatz kostet heute wenig – Daten zu verlieren kann hingegen sehr teuer werden.

3. Daten kopieren
Eine forensische Sicherung unterscheidet sich von einer gewöhnlichen Kopie durch die zusätzliche Sicherung aller Metadaten, dem elektronischen Fingerabdruck einer Datei. Wird eine Datei beispielsweise kopiert und daraufhin erneut abgespeichert, trägt die Kopie ein anderes Erstelldatum. Derartige elektronische Informationen können aber ein wichtiges Beweismittel sein, deren Veränderung nicht nur den Beweis verändert, sondern zudem die Validität aller anderen Meta-Daten (Autor, zuletzt geöffnet, gedruckt, versandt, kopiert) in Frage stellt.
Bei großen Datenmengen, Laptop- und Handysicherungen ist es sinnvoll, einen IT-Forensiker hinzuzuziehen, der bei der Identifizierung und Sammlung relevanter Daten hilft und als Sachverständiger vor Gericht auftreten kann.

4. Gelöschte Daten übersehen
Besonderes Augenmerk gilt mutwillig oder versehentlich gelöschten Daten. Denn wer den Papierkorb leert, gibt lediglich den belegten Speicherplatz für ein erneutes Überschreiben frei. Die frei gegebenen Bereiche und damit auch die darin enthaltenen Daten werden jedoch mit den richtigen forensischen Tools – hier seien EnCase und FTK Imager als zwei der gängigsten genannt – wiederherstellbar. Mit dem erhaltenen „Full Image" kann so jederzeit auf den IST-Zustand zum Zeitpunkt der Datensammlung zurückgegriffen werden.

5. Suchen in Outlook
Die Suchfunktion von Outlook oder anderen E-Mail-Programmen zum Auffinden bestimmter Informationen liefert äußerst unvollständige Ergebnisse. So zeigt Outlook nur eine begrenzte Anzahl von Ergebnissen an und auch nur die Daten, die aktuell auf dem System verfügbar sind und ignoriert Dokumente, die nicht identifizierbar sind, z.B. vom System bereits archivierte Nachrichten, gescannte Anhänge oder Bilder.

Fazit

Forensische Datensicherungen sind komplex, zeitaufwändig und benötigen erhebliches Wissen, um erfolgreich durchgeführt werden zu können. Es geht nicht nur um den Inhalt der Daten, sondern auch um eine gerichtsfeste Beweismittelsicherung. Dazu gehören Metadaten und eine lückenlose Beweismittelkette, erstellt durch ausgebildete Experten. Je früher mit der professionellen Planung begonnen wird, desto weniger Fehler geschehen. Und desto besser können sich Unternehmen und Kanzleien auf die Ergebnisse der Untersuchung vorbereiten.

Hinweis zum Autor:

Daniel Heinrichs
arbeitet bei KLDiscovery im Bereich der Computerforensik und Ediscovery und betreut in seiner Rolle als Business Development Manager Unternehmen und Kanzleien in Deutschland, Österreich und der Schweiz. Herr Heinrichs hat einen Abschluss als Master in Business Management.

Datenschutz 2020

Bewährte Arbeitshilfen für alle Praktiker

Dokumentation zum Datenschutz
mit Informationsfreiheitsrecht

Wissenschaftlich betreut von Professorin Dr. Indra Spiecker gen. Döhmann, LL.M., redaktionell betreut und bearbeitet von Dr. Sebastian Bretthauer.

2020, Fortsetzungswerk in 6 Ordnern, ca. 8.000 S., jetzt nur 178,– € statt 258,– €
ISBN 978-3-8487-5000-9

NEU 2020

Bundesdatenschutzgesetz
Handkommentar

Herausgegeben von Prof. Dr. Gernot Sydow

2020, 909 S., geb., 128,– €
ISBN 978-3-8487-4999-7

2. DSAnpUG-EU schon berücksichtigt!

NEU 2020

Landesdatenschutzgesetz Rheinland-Pfalz
Handkommentar

Herausgegeben von Prof. Dr. Dieter Kugelmann

2020, 608 S., geb., 98,– €
ISBN 978-3-8487-5428-1

NEU 2020

Landesdatenschutzgesetz Nordrhein-Westfalen
Handkommentar

Herausgegeben von Prof. Dr. Rolf Schwartmann und Prof. Dr. Heinz-Joachim Pabst

2020, 672 S., geb., 98,– €
ISBN 978-3-8487-6308-5

NEU 2020

Landesdatenschutzgesetz Baden-Württemberg
Handkommentar

Herausgegeben von Dr. Alfred G. Debus und Dr. Corinna Sicko

2020, ca. 300 S., geb., ca. 68,– €
ISBN 978-3-8487-5725-1
Erscheint ca. Oktober 2020

NEU 2020

Landesdatenschutzgesetz Niedersachsen
Handkommentar

Herausgegeben von Prof. Dr. Tina Krügel, LL.M., und Prof. Dr. Fabian Schmieder

2020, ca. 500 S., geb., ca. 98,– €
ISBN 978-3-8487-5692-6
Erscheint ca. Oktober 2020

Bestellen Sie im Buchhandel oder versandkostenfrei online unter nomos-shop.de
Bestell-Hotline (+49)7221.2104-37 | **E-Mail** bestellung@nomos.de | **Fax** (+49)7221.2104-43
Alle Preise inkl. Mehrwertsteuer

Nomos

Retuschiert die DSGVO die Möglichkeit zur Fotonutzung?

Nach dem Fotografen *Ansel Adams* gibt es *„nichts Schlimmeres als ein brillantes Bild eines schlechten Konzepts“*. Dieser Grundsatz gilt nicht nur für die Fotografie im Allgemeinen, sondern auch für den datenschutzrechtlichen Umgang mit Bildaufnahmen. Die Zeiten, in denen Unternehmen Fotografien von Beschäftigten einfach verwenden können, sind längst vorbei. Der Weg vom Konzept zum Bild ist heute aufgrund der neuen Rechenschaftsverpflichtung nach Art. 5 Abs. 2 Datenschutzgrundverordnung (DSGVO) der Weg vom Konzept zum Bild, dokumentiert in einer Richtlinie zur Verwendung von Beschäftigtenfotografien für jede Art von Bild - egal ob brillant oder weniger brillant.

Gerade aber die Erstellung dieser unternehmensweiten Richtlinien zur Verwendung von Beschäftigtenfotografien ist für Unternehmen eine erhebliche Herausforderung. Erschwerend ist dabei zu berücksichtigen, dass gefestigte Grundsätze zur Verwendung von Beschäftigtenfotografien, wie sie etwa durch das Urteil des BAG vom 11. Dezember 2014[1] innerhalb des Anwendungsbereichs des KUG/BDSG a.F. festgelegt wurden, nur noch bedingt als Orientierung genutzt werden können. Insbesondere die höchstrichterlich geprägte Möglichkeit zur Einschränkung des Widerrufs der Einwilligung ist heute bedenklich und nicht mehr ratsam.[2]

Da Fotografien personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO sind und damit dem Anwendungsbereich der DSGVO unterfallen, muss bei der Verarbeitung von Fotografien auf die Rechtsgrundlagen der DSGVO zurückgegriffen werden.[3] Zur Rechtfertigung kommen maßgeblich die Einwilligung der betroffenen Personen nach Art. 6 Abs. 1 Satz 1 lit. a DSGVO und das berechtigte Interesse des Unternehmens nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO in Betracht. Während die jederzeit widerrufliche Einwilligung für jeden Beschäftigten gesondert dokumentiert werden muss, ist im Kontext des Art. 6 Abs. 1 Satz 1 lit. f DSGVO eine Interessenabwägung samt Widerspruchsmöglichkeit je Unternehmen zu dokumentieren. Hierbei bietet sich jedenfalls ein ergänzender Rückgriff auf bekannte und bewährte Auslegungsgrundsätze des KUG an.[4]

Betriebsintern ist zudem an § 26 BDSG n.F. zu denken. Ist die Verarbeitung der Fotografie für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnis erforderlich (§ 26 Abs. 1 Satz 1 Var. 2, Var. 3 BDSG n.F.), liegt eine weitere Rechtsgrundlage vor.[5] Ein denkbarer Anwendungsfall ist dabei das zu Verifizierungszwecken erforderliche Foto auf dem Betriebsausweis.

Nach Auffassung von Aufsichtsbehörden ist die Einwilligung die zentrale Rechtsgrundlage für die Verarbeitung von Fotografien. Ob daneben auch ein berechtigtes Interesse des Unternehmens Bestand hat, wird von Aufsichtsbehörden unterschiedlich bewertet. Während sich die Landesbeauftragten Rheinland-Pfalz und Baden-Württemberg dahingehend positionieren, dass „[…] *kein Weg an der Einwilligung des Abgebildeten* [vorbeiführe]“[6], geht das Bayerische Landesamt für Datenschutzaufsicht davon aus, dass eine Veröffentlichung von Beschäftigtenfotografien im Internet auch nach einer entsprechenden Interessenabwägung zulässig sei.[7] Ein Weg, den die Praxis immer mehr aufgreift, um dem „eigenen Bilderchaos“ zu entkommen!

Regelrecht dankbar können Unternehmen sein, dass das ULD Schleswig-Holstein in alter Tradition weiterhin davon ausgeht, dass die Einwilligung im Beschäftigtenverhältnis keinen Bestand haben könne, da es stets an der Freiwilligkeit mangle.[8] Im Umkehrschluss bleibt dann aber nur noch der Rückgriff auf das berechtigte Interesse, sofern man Unternehmen das Recht zur Verarbeitung von Beschäftigtenfotografien nicht in Gänze absprechen möchte. Bundesweit ist damit gewiss, dass derzeit nichts gewiss ist: Eine einheitliche Linie der Aufsichtsbehörden zur Verwendung von Fotografien ist nicht erkennbar, höchstrichterliche Rechtsprechung zur Auslegung der potentiellen Rechtsgrundlagen fehlt bislang. Was also tun, um weiter fotografieren zu können, aber dennoch Bußgelder zu vermeiden?

Dieser Weg ist bundesweit durch viele Unternehmen geebnet, die sich in diesem Kontext bereits aufgestellt haben. Es braucht ein durchdachtes, dokumentiertes sowie implementiertes Konzept, welches Datenschützer „Richtlinie zur Verwendung von Beschäftigtenfotografien“ nennen. Dabei müssen Fotografien zunächst in sog. „Cluster“ eingeordnet werden. Diese Cluster benennen Art des Bildes, Verwendungszweck und das Veröffentlichungsmedium. Wenige Cluster werden ausnahmslos mit einer Einwilligung rechtskonform umsetzbar sein (Portraitfotos, gezielte Aufnahmen der betroffenen Person, etc.). Viele andere Veröffentlichungen können hiervon abweichend auf das berechtigte Interesse gestützt werden („Beiwerk“, Gesamtgeschehen intern/extern, Personen des öffentlichen Lebens, etc.). Zudem sollte klar und leicht verständlich festgehalten werden, wie betroffene Personen vorab zu informieren sind (schriftlich, Aushang, E-Mail, Webseite, QR-Code), wie die Freiwilligkeit durch frühestmögliche Information belegt und wie zwischen einwilligenden und nicht einwilligenden Personen bei Veranstaltungen differenziert wird.

Die Erfahrungen der vergangenen Jahre zeigen, dass Konzepte und Richtlinien durch Aufsichtsbehörden begünstigend berücksichtigt werden. Darüber hinaus ist absehbar, dass sich auch Gerichte zunehmend mit der (rechtswidrigen) Veröffentlichung etwaiger Fotografien beschäftigen werden. Dass Unternehmen auch in Zukunft lediglich Schadenersatzforderungen in Höhe von EURO 1.000,00 befürchten müssen[9], ist abwegig – zumal der erheblich höhere Bußgeldkatalog der DSGVO droht.

Hinweis zu den Autoren:

RA Markus Säugling
ist Gründungspartner von MAGELLAN Rechtsanwälte mit mehr als 18 Jahren Erfahrung in der Datenschutzberatung. Er berät Konzerne branchenübergreifend und ist bundesweit als Dozent für renommierte Ausbildungsinstitute tätig.

RA Rouven K. Schäfer
ist Senior Associate bei MAGELLAN Rechtsanwälte und berät datenschutzrechtlich mit Schwerpunkt im Bereich Direktmarketing und Vertrieb.

RA Dr. Martin Scheurer
ist Senior Associate bei MAGELLAN Rechtsanwälte und berät schwerpunktmäßig im Bereich Gesundheits- und Beschäftigtendatenschutz. Darüber hinaus publiziert er regelmäßig zu aktuellen Fragen des Datenschutzrechts.

[1] BAG, Urt. v. 11.12.2014 – 8 AZR 1010/13, NZA 2015, 604 ff.
[2] In diesem Sinne auch der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Ratgeber Beschäftigtendatenschutz, 4. Aufl. 2020, S. 43 ff.
[3] Vgl. dazu etwa jüngst ArbG Lübeck, Beschl. v. 20.06.2019 – 1 Ca 538/19, BeckRS 2019, 36456 Rn. 24; *Faulhaber/Scheurer*, jM 2019, 2.
[4] So auch LG Frankfurt am Main, Urt. v. 26.09.2019 – 2-03 O 402/18, ZD 2020, 204 Rn. 61 m. w. N.
[5] Vgl. dazu etwa *Assmus/Winzer, ZD 2018, 508, 511 ff.*
[6] So ausdrücklich der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Ratgeber Beschäftigtendatenschutz, 4. Aufl. 2020, S. 42; in diesem Sinne auch der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Rechtliche Anforderungen beim Fotografieren unter der DS-GVO.
[7] BayLDA, FAQ „Dürfen Fotos von Mitarbeitern, Vereinsmitgliedern oder Dritten auf der Webseite veröffentlicht werden?“.
[8] ULD, Praxisreihe 6 Fotos und Webcams, 2019, S. 12.
[9] ArbG Lübeck, Beschl. v. 20.06.2019 – 1 Ca 538/19.

Sichere Kanzleisoftware

Worauf man beim Kauf achten sollte

Kanzleien verarbeiten sensible Daten. Deshalb muss Datenschutz bei der Entscheidung für eine Kanzleisoftware von Anfang an einen besonderen Stellenwert einnehmen. Und das schon bei der Softwareentwicklung. Nur so können die Sicherheit sensibler Mandanten-Daten gewährleistet und die Anforderungen der DSGVO erfüllt werden. Für den rechtssicheren und datenschutzkonformen Umgang mit diesen Daten ist die Kanzlei immer selbst verantwortlich.

Datenschutz von Anfang an

Seit Inkrafttreten der DSGVO hat sich das Thema Datenschutz stärker im Bewusstsein der Wirtschaft und beratender Anwälte verankert. Auch wenn es ihn schon vor dem 25.05.2018 gab, hat niemand darüber gesprochen. Heute ist das Thema in aller Munde. Mit dem Wirksamwerden der DSGVO veränderten sich die auch die Anforderungen an Kanzleien stark. Der Betroffene, die Person, die ihre Daten zur Verarbeitung überlässt, steht im Zentrum. Hauptthema: die digitale Verarbeitung der Daten – Data Protection by Design und Data Protection by Default. Die DSGVO widmet diesen zentralen Prinzipien des Datenschutzes sogar einen eigenen Artikel: Artikel 25. Das unterstreicht die Wichtigkeit der Betroffenenrechte als zentralen Ausgangpunkt aller Regelungen rund um den Datenschutz.

Die Verordnung lässt im Einzelnen offen, was genau zu tun ist. Allerdings erklärt sie, was das für den Einsatz von Datenverarbeitungsverfahren bedeutet: Sie sollen dem „Stand der Technik" entsprechen und den Verantwortlichen dazu in die Lage versetzen, seinen Datenschutzverpflichtungen nachzukommen (Art 25/32 DSGVO und Erwägungsgrund 78).

Worauf beim Kauf von Kanzleisoftware zu achten ist

Nicht neu ist, dass technische Standards beim Einsatz von Software die Datensicherheit gewährleisten sollen. Neu ist aber, dass sich diese Anforderungen von der Erhebung bis zur Löschung an den Rechten der betroffenen Personen orientieren sollen. Das bedeutet, dass bereits in der Planungsphase folgende Fragen berücksichtigt werden müssen:

- Wie kann ich die Rechtevergabe in meiner Software steuern?
- Kann ich Datensätze einschränken und kann ich sie nachweisbar löschen?
- Wie verwalte ich die verarbeiteten Daten von der Erfassung bis zum Abschluss so, dass der Zugriff immer den beabsichtigten Zwecken entspricht?
- Ist meine Software auch auf die Arbeit im Homeoffice ausgelegt?

Das ist nur ein kleiner Ausschnitt aus einem großen Portfolio relevanter Fragestellungen im Sinne der DSGVO. Denn bei Beschwerden von Betroffenen oder Prüfhandlungen der Aufsichtsbehörden wird die Frage, ob die gewählte Lösung alles kann, was sie können muss, zur bußgeldbewährten Quizfrage.

Konsequenzen für Kanzleien ohne sichere Software

Manchmal spielt es nicht nur eine Rolle, ob eine Anforderung irgendwie über drei Umwege nachgewiesen werden kann. Es geht auch darum, ob sie es „benutzerfreundlich“ kann. Betroffenen soll es jederzeit leicht gemacht werden, Auskünfte zu bekommen, Benutzer sollen ohne komplizierte Operationen Schutzmaßnahmen durch Einstellungen vornehmen oder einen Lösch- bzw. Einschränkungsvorgang auf den Weg bringen können. Hinter dem Prinzip „Data Protection by Default“ verbirgt sich die Erwartung, dass solche Einstellungen nach Möglichkeit antizipieren, was an Datenschutzmaßnahmen erforderlich ist.

Diese dem Erwerber der Software mit Art. 25 auferlegte Pflicht ist umso leichter zu erfüllen, je mehr die ausgewählte Lösung bereits brauchbare Strategien anbietet, um in der jeweiligen Situation richtig zu reagieren.

Dass das manchmal gar nicht so leicht ist, zeigt sich am Beispiel des **höchsten Bußgeldes** seit Inkrafttreten der DSGVO. Es wurde in Höhe von 14,5 Millionen Euro gegen eine Wohnungsgesellschaft verhängt. Diese hatte versäumt dafür zu sorgen, dass das von ihr angewendete Archivsystem auch die Löschung von Daten vorsieht. Klingt fast zu einfach, ist aber wahr. Wahr ist auch, dass ein hoher Prozentsatz an Rechtsanwaltskanzleien diese Themen immer weit nach hinten schiebt. Fragen danach, wie und wann Daten einzuschränken sind, wann welche Daten zu löschen sind und wie ich diese Informationen für den Betroffenen bereithalten kann, bleiben häufig unbeantwortet. Dass und wie die geeignete Softwareanwendung unterstützen kann, wird dadurch umso wichtiger. Wenn die Anwendung in der Lage ist, meine Anforderungen bereits so abzubilden, dass die DSGVO-Konformität gewahrt ist, muss der Verantwortliche sich nicht mit Themen auseinandersetzen, für die er ungerne Zeit erübrigt.

Fazit: Seien Sie kritisch beim Softwarekauf. Scheinbar unscheinbare Probleme können zu mächtigen Konsequenzen führen, wenn eine Entscheidung zum Einsatz eines Datenverarbeitungsverfahrens nicht wohl überdacht ist. Es empfiehlt sich, beim Hersteller aktiv nachzufragen, Datenschutzfeatures zu hinterfragen. Beim Kauf und bei der Planung zum Einsatz einer Software sollten Kanzleien sich überlegen: Auf was muss ich vorbereitet sein und wie leicht macht es mir die vorgestellte Software?

Hinweis zum Autor:

Diplom-Kaufmann Fritz Spaeder
ist Head of Consultants bei der STP AG. Er berät Rechtsanwaltskanzleien in Organisationsfragen und unterstützt Zertifizierungsvorhaben in Kanzleien. Er ist Systemischer Coach und zertifizierter Datenschutzbeauftragter (IHK). Als externer Datenschutzbeauftragter ist er derzeit in mehr als 20 Kanzleien aktiv.

Privacy Tech – technologieunterstütztes Datenschutzmanagement

Datenschutzrechtliche Compliance gewinnt zunehmend an Bedeutung, weshalb ein geeignetes Datenschutzmanagementsystem unbedingt empfehlenswert ist. Hier bietet der Einsatz digitaler und automatisierter Lösungen große Vorteile. Dieser Beitrag analysiert das breite und schnell wachsende Angebot an Privacy-Tech-Lösungen mit Blick auf neue Standards und deren Praxisnutzen.

I. Vorgaben der DSGVO

Mit Einführung der DSGVO wurden die Dokumentations-, Nachweispflichten und Informationspflichten deutlich umfangreicher ausgestaltet. Hervorzuheben sind die allgemeinen Nachweispflichten des Verantwortlichen (Art. 5 I DSGVO und Art. 24 I DSGVO): Der Verarbeiter muss die Vorgaben der DSGVO nicht nur einhalten, sondern auch präventiv deren Einhaltung nachweisen können (umfassende Rechenschaftspflicht). Zudem erfordern Informationspflichten (Art. 12 ff. DSGVO) eine systematische Dokumentation verarbeitungsbezogener Details, welche Nutzern und anderen Betroffenen mitzuteilen sind. Fast jedes Unternehmen ist zudem verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) zu führen.

Um die Rechtmäßigkeit der Datenverarbeitung belastbar nachweisen zu können, ist deshalb die Implementierung eines geeigneten Datenschutzmanagementsystems unverzichtbar. Vor diesem Hintergrund kann Privacy Tech durch digitale und automatisierte Lösungen entscheidende Vorteile bringen. Dabei ist die Auswahl des richtigen Systems nicht nur eine wirtschaftliche Frage, sondern entscheidet unmittelbar über die Wirksamkeit des Datenschutz- und Risikomanagements sowie den Erfolg von Geschäftsmodellen.

II. Privacy Tech – digitales und automatisiertes Datenschutzmanagement

Als Privacy Tech werden Tools bezeichnet, die Unternehmen bei der Einhaltung datenschutzrechtlicher Pflichten mit digitalen und automatisierten Workflows unterstützen. Solche Werkzeuge können sowohl Datenschutzexperten unterstützen als auch Laien dazu befähigen, ein angemessenes Datenschutzmanagement aufzubauen und Risiken zu identifizieren.

Die individuelle Erstellung und Pflege von Verzeichnissen und Dokumentationen in Texten, Tabellen oder analogen Dokumenten war lange verbreitet. Der Aufbau eines Datenschutzmanagements auf dieser Basis ist zwar möglich, erfordert aber einen hohen Aufwand und ist fehleranfällig. Verfügt ein Unternehmen nicht über ausreichende Ressourcen und fehlt es an Datenschutzwissen, etwa weil kein Datenschutzbeauftragter zur Verfügung steht, können digitale und automatisierte Konzepte entscheidende Vorteile bieten und dabei helfen, ein angemessenes Datenschutzmanagement zu etablieren und aktuell zu halten.

1. Typen und Funktionen verfügbarer Lösungen

Auf dem Markt ist ein breites, ständig wachsendes Angebot digitaler Lösungen verfügbar. Zählte die International Association of Privacy Professionals (IAPP) in ihrem jährlich erscheinenden Vendor Report im Jahre 2017 noch 44 Lösungen, sind es 2020 bereits über 300. Welche Lösung für welches Unternehmen geeignet ist, hängt von verschiedenen Faktoren, wie insbesondere dem Verwendungszweck und den verfügbaren Ressourcen ab.

a. Dokumentation

Eine von Privacy-Tech-Lösungen häufig angebotene Funktion ist die Bereitstellung von Dokumentationstools. Über geführte Workflows, die mit Blick auf komplexe rechtliche Vorgaben entwickelt wurden, können datenschutzrelevante Sachverhalte zielgerichtet dokumentiert werden. Je detaillierter Informationen dokumentiert werden sollen, desto mehr Ressourcen und Fachwissen erfordern die Implementierung und der Einsatz solcher Tools – sofern die komplexen datenschutzrechtliche Anforderungen durch die Privacy-Tech-Anbieter nicht angemessen auf das für den jeweiligen Anwender erforderliche Maß heruntergebrochen werden.

b. Einwilligungs- und Betroffenenrechtemanagement

Regelmäßig sehr wichtig ist der Aufbau eines zuverlässigen Einwilligungsmanagements, etwa im Marketingbereich. Für Einwilligungen als Rechtsgrundlage einer Datenverarbeitung (Art. 6 Abs. 1 lit. a DSGVO) bestehen hohe Anforderungen an das Datenschutzmanagement: Die Prozesse der Einholung, der Speicherung, der Dokumentation und des Nachweises sowie der Berücksichtigung von Widerrufen müssen bedacht werden. Ferner erfordert die frist- und formgerechte Erfüllung von Betroffenenrechten wie Auskunftsersuchen und Löschungsverlangen ein passgenaues unternehmensweites Konzept.

Privacy Tech bietet verschiedene Konzepte zur Abbildung und Automatisierung dieser Prozesse. Insbesondere wenn Einwilligungen über elektronische Kommunikation eingeholt werden, sind sog. Consent-Management-Lösungen empfehlenswert. Der BGH hat die strengen Anforderungen an das Einwilligungsmanagement auf Websites, häufig in Gestalt sogenannter Cookie-Banner, zudem erst kürzlich bestätigt (Urt. v. 28.5.2020 – I ZR 7/16) – der Einsatz einer Consent-Management-Lösung drängt sich also auf. Für den praxisrelevanten Bereich der Betroffenenrechte bieten sich ebenfalls digitale und automatisierte Lösungen an.

c. Vorlagen, Informationen und Anleitungen

Das Datenschutzrecht wurde durch die DSGVO europaweit vereinheitlicht, Öffnungsklauseln lassen jedoch beachtliche Spielräume für den nationalen Gesetzgeber. In Deutschland wurde hiervon durch die Neuregelung des Bundesdatenschutzgesetzes (BDSG) sowie durch spezialgesetzliche Regelungen, etwa im Handels-, Sozial- und Steuerrecht Gebrauch gemacht. Überdies ist das Datenschutzrecht in hohem Maße auslegungsbedürftig,

etwa bei praxisrelevanten Fragestellungen wie der Festlegung konkreter Lösch- und Aufbewahrungsfristen, dem angemessenen Umfang technischer und organisatorischer Maßnahmen (TOM) sowie zu erteilender Datenschutzinformationen. Nationale und europäische Behörden und Institutionen haben eine Fülle von Dokumenten zur Auslegung datenschutzrechtlicher Vorgaben sowie Vorlagen zur praktischen Umsetzung veröffentlicht. Auch die Rechtsprechung beschäftigt sich fortlaufend mit datenschutzrechtlichen Fragestellungen.

In Ansehung der Vielzahl von Rechts- und Informationsquellen sowie den teilweise abweichenden Auslegungen und häufig wenig praxisnahen Vorlagen sowie Vorgaben bietet der digitale Datenschutzmarkt vielversprechende Lösungen: Privacy-Tech-Tools können durch die Bereitstellung von Vorlagen, Informationen und Anleitungen dabei unterstützen, ein optimales Datenschutzmanagement aufzubauen und den individuellen Anforderungen entsprechende Lösungen zu finden.

d. Automatisierung

Die Automatisierung von rechtlichen Arbeitsprozessen, häufig auch als Legal Tech bezeichnet, eröffnet im Datenschutzbereich großes Potential. Privacy-Tech-Tools bieten eine automatisierte Bewertung dokumentierter oder ausgelesener Informationen an; Anwendungsfälle reichen von automatisierten Risikoabwägungen und Datenschutz-Folgenabschätzungen bis hin zur Bewertung von Datenschutzverletzungen oder Berechnung von Aufbewahrungsfristen. Daneben stehen Werkzeuge zur Verfügung, die die Sicherheit von Websites oder Schnittstellen automatisiert analysieren und bewerten. Schließlich können Add-ons für bestehende Datenverarbeitungssoftware unter anderem zur Umsetzung automatisierter Löschroutinen eingesetzt werden.

e. Integrierte Lösungen

Bei integrierten Lösungen handelt es sich um Kombinationen der vorgenannten Ansätze, wobei insoweit häufig auch Beratungsleistungen angeboten werden. Im Idealfall können Unternehmen alle erforderlichen datenschutzrechtlichen Dokumentationen in einer einzigen Software abbilden, Maßnahmen daraus ableiten und somit ein effizientes digitales Datenschutzmanagement aufbauen, das sich ressourcenfreundlich implementieren lässt.

2. Ausrichtung und Praxisnutzen

Aufgrund der Bandbreite verfügbarer Lösungen bietet Privacy Tech grundsätzlich stets Vorteile, sofern das gewählte System die betrieblichen Anforderungen trifft und rechtliche Vorgaben zuverlässig abbildet, ohne sie unzulässig zu vereinfachen. Entscheidend für den Praxisnutzen einer digitalen Datenschutzsoftware sind alle Umstände der Verarbeitung personenbezogener Daten. Umfangreiche, komplexe Tools, die nur von Experten bedient werden können, bietet häufig nur geringen Mehrwert für kleine und mittlere Unternehmen. Bei großen Unternehmen müssen Besonderheiten, wie etwa internationale Datenübermittlungen, datenintensive Geschäftsmodelle oder risikoreiche Verarbeitungen, berücksichtigt werden – und erfordern vielfach eine individuelle Beratung.

3. Einbindung von Experten

Beratung durch Datenschutzexperten wird durch Privacy Tech somit keinesfalls verzichtbar. Ist spezifisches Fachwissen erforderlich, sollte z. B. ein Datenschutzbeauftragter zur Verfügung stehen oder entsprechende Beratung bereits Leistungsbestandteil des Privacy-Tech-Tools sein. Unpassende Lösungen führen hier nicht nur zu vermeidbaren Kosten, sondern bringen auch hohe Risiken mit sich. Denn unabhängig vom Einsatz von Privacy Tech verbleibt die Pflicht zur Umsetzung angemessener Datenschutzmaßnahmen (und damit die Haftung) bei dem Verantwortlichen, mithin der Geschäftsführung. Vertraut werden sollte daher nur solchen Datenschutzlösungen, die durch Experten entwickelt und fortlaufend aktualisiert werden.

III. Zusammenfassung und Ausblick

Privacy Tech verändert in Ansehung der mit der DSGVO gestiegenen rechtlichen Anforderungen den Bereich des Datenschutzes. Digitales und automatisiertes Datenschutzmanagement bietet hier große Vorteile, indem der Aufbau eines effizienten sowie wirtschaftlichen Datenschutzmanagementsystems unterstützt und Prozessvereinfachung ermöglicht wird. Zwar ist eine vollständige Automatisierung des Datenschutzmanagements aktuell nicht realistisch; es ist aber absehbar, dass sowohl das Angebot an als auch die Nachfrage nach digitalen Datenschutzlösungen weiter wachsen werden.

Im Idealfall definieren digitale Datenschutzlösungen den für den Anwender passenden Rahmen und schonen (finanzielle und personelle) Ressourcen. Soweit die gesetzlichen und behördlichen Vorgaben fortlaufend berücksichtigt werden, kann Privacy Tech auch solche Unternehmen bei der Etablierung angemessener Datenschutzkonzepte unterstützen, die individuelle Datenschutzmanagementsysteme bisher nicht umsetzen konnten (oder wollten). Insgesamt gilt, dass – wenn die gewählten Systeme zu den betrieblichen Anforderungen passen – Privacy Tech sowohl den Schutz personenbezogener Daten als auch die Umsetzung von datenschutzrechtlicher Compliance für eine Vielzahl von Unternehmen spürbar erleichtert.

Hinweis zu den Autoren:

Alexander Ingelheim
ist Datenschutzbeauftragter und geschäftsführender Gründer des Privacy-Tech-Dienstleisters PROLIANCE GmbH (datenschutzexperte.de), die unter anderem die Datenschutzmanagementplattform proliance360 anbietet.

Prof. Dr. Boris P. Paal,
M. Jur. (Oxford) ist Direktor des Instituts für Medien- und Informationsrecht, Abt. I: Privatrecht an der Albert-Ludwigs-Universität Freiburg und wissenschaftlicher Beirat der PROLIANCE GmbH.

DSGVO: Spielregeln im Bußgeldverfahren

Der neue Leitfaden

Härting/Konrad
DSGVO im Praxistest
Ermittlungen Bußgelder Verfahren
Bearbeitet von RA Prof. Niko Härting und RA Lasse Konrad. Lexikonformat, brosch., 148 Seiten, 39,80 €.
ISBN 978-3-504-56078-2

Das Werk online
otto-schmidt.de/bmds
juris.de/pmds

Inzwischen sind die ersten Bußgelder in Millionenhöhe für Datenschutzverstöße verhängt worden. Höchste Zeit also für Unternehmen und ihre Berater, sich mit den Spielregeln für eine Auseinandersetzung mit den Aufsichtsbehörden vertraut zu machen. Die Autoren beantworten in diesem neuen Werk 249 Fragen, die sich in aufsichtsbehördlichen Verfahren und datenschutzrechtlichen Gerichtsprozessen stellen können. Das Augenmerk liegt dabei weniger auf dem Datenschutzrecht als auf dem Verfahrens- und Prozessrecht.

Damit erhält der Praktiker eine ausführliche Handlungsanleitung für und gegen aufsichtsbehördliche Maßnahmen. In drei Teilen werden die Phasen einer Eskalation behandelt: Welche Kompetenzen hat die Aufsichtsbehörde bei Auskunftsersuchen und Vor-Ort-Prüfung? Welche Sanktionen dürfen wie verhängt werden (Verbot, Anordnung, Bußgeld, etc.)? Welche prozessualen Möglichkeiten gibt es vor Verwaltungs- und Strafgerichten?

Gratis-Leseprobe und Bestellung **www.otto-schmidt.de**

ottoschmidt