Infos zur Datenschutzverordnung
Auch Kleinunternehmen betroffen

Mit Inkrafttreten des in der Europäischen Union einheitlich geltenden Datenschutzrechts ›DS-GVO‹ am 25. Mai 2018 wurde ein Gesetzeswerk geschaffen, das für Unternehmen und Vereine massive Veränderungen bringt. Jeder dort Verantwortliche sollte sich daher intensiv mit diesem Gesetz befassen, da deren Nichtbeachtung massive Strafen nach sich zieht.

Wer personenbezogene Daten elektronisch, und sei es nur mit einem einzigen PC, oder mit einem geordneten Karteisystem verarbeitet, ist verpflichtet, dies nach den Regeln des neuen Datenschutzrechts ›DS-GVO‹ vorzunehmen. Dabei spielt es keine Rolle, was mit den personenbezogenen Daten geschieht – es handelt sich stets um ein Verarbeiten im Sinn des neuen Datenschutzrechts ›DS-GVO‹. Die einzige Ausnahme ist die Verarbeitung für ausschließlich persönliche und familiäre Tätigkeiten. Dies fällt nicht in den Bereich des DS-GVO.

Unternehmen und Vereine sind demnach verpflichtet, ein Verzeichnis über alle Verarbeitungstätigkeiten rund um die Verwendung personenbezogener Daten zu führen und zudem laufend zu dokumentieren, in welchem Zusammenhang mit diesen Daten gearbeitet wird.

Dabei ist wichtig, zu wissen, dass personenbezogene Daten alle Informationen sind, die sich auf eine natürliche Person beziehen und die mittels Zuordnung zu einer Kennung, wie etwa Namen, Kennnummer, Standortdaten oder anhand besonderer Merkmale, wie etwa psychische, wirtschaftliche, kulturelle oder soziale Eigenschaften identifiziert werden kann.

Ohne Ausnahme

In der Verordnung gibt es zwar eine Freistellung von der Verpflichtung, die DS-GVO zu beachten, wenn weniger als 250 Mitarbeiter beschäftigt werden, doch hat dies in der Praxis keinerlei Bedeutung, da diese Freistellung unter anderem nur dann gilt, wenn die Datenverarbeitung nur gelegentlich erfolgt. Dies ist bei keinem noch so kleinen Unternehmen der Fall, da beispielsweise kontinuierlich Lohnabrechnungen durchgeführt werden. Auch kleinste Vereine sind davon betroffen, da diese in der Regel eine Mitgliederverwaltung regelmäßig aktualisieren, um Zu- und Abgänge zu erfassen. Zum Nachweis des korrekten Umgangs mit personenbezogenen Daten, ist eine Dokumentation zu erstellen, aus der hervorgeht, welche Daten von wem verarbeitet werden, auf welcher Rechtsgrundlage dies geschieht und wie lange die Daten gespeichert werden. Die Angaben müssen aussagekräftig sein. Diese bedeutet, dass sie umso detaillierter sein müssen, je größer ein Unternehmen oder ein Verein ist. Diese Dokumentation hat den Zweck, gegenüber der Aufsichtsbehörde nachzuweisen, dass Daten von Mitarbeitern, Kunden, Lieferanten oder Vereinsmitgliedern korrekt verarbeitet werden.

Die Verordnung zwingt die Verantwortlichen zu einer akribischen Vorgehensweise. Es genügt laut DS-GVO nicht, Änderungen an der Dokumentation einfach durch Überschreiben der bestehenden Inhalte vorzunehmen. Vielmehr muss eine Kopie der aktuellen Datei angefertigt werden, ehe diese mit neuen Inhalten gefüttert wird. Die angefertigten Kopien sind mindestens ein Jahr aufzubewahren, um nachweisen zu können, was in diesem Zeitraum verändert wurde.

Von allen in der Adressdatei stehenden Personen muss eine Einwilligung zur Verarbeitung der persönlichen Daten vorliegen. Ist dies nicht der Fall, so muss diese umgehend eingeholt werden, ansonsten sind die Daten zu löschen. Beim Einholen der Einwilligung ist das Anschreiben so zu gestalten, dass der betroffenen Person klar dargelegt wird, zu welchem Zweck die Daten verarbeitet werden und dass diese Einwilligung jederzeit widerrufen werden kann.

Mitarbeiter schulen

Nicht vergessen werden darf, die Mitarbeiter auf eine gesetzeskonforme Verarbeitung der Ihnen anvertrauten personenbezogenen Daten zu verpflichten. Beispielsweise dürfen die gewonnen Adressdaten nicht für jeden Zweck verwendet werden. Wird beispielsweise ein Auto

verkauft, dürfen Kunden nur Werbung rund ums Auto bekommen, nicht jedoch Werbung etwa zu Busreisen. Eine Weitergabe der Daten an ein Busunternehmen ist demnach nicht zulässig, da dieses Unternehmen mit dem ursprünglichen Autokauf nichts zu tun hat. Abgesehen davon, müssen Verantwortliche dafür sorgen, dass die Daten ihrer Kunden stets aktuell sind. Darüber hinaus sind sie zu löschen, wenn sie nicht mehr benötigt werden. Zumindest müssen sie so verändert werden, dass ein Personenbezug wegfällt.

Werden externe Unternehmen etwa zur Lohnbuchhaltung oder zur Adressenverarbeitung beauftragt, so muss der Auftraggeber prüfen, ob die Datenverarbeitung nach den datenschutzrechtlichen Vorschriften erfolgt. Er haftet sonst für ein eventuelles Fehlverhalten. Daher wird von Juristen empfohlen, dass sich der Auftraggeber umfangreiche Kontrollrechte einräumen lässt, die es ihm ermöglichen, ohne Vorankündigung Kontrollen vor Ort durchzuführen.

Auf IT-Sicherheit achten

Das DS-GVO legt ein besonderes Augenmerk auf die IT-Sicherheit. Gefordert werden Vertraulichkeit, Integrität und jederzeitige Verfügbarkeit der Systeme. Es geht also darum, Informationen vor Unbefugten zu verbergen, deren Unversehrtheit sicherzustellen und sie jederzeit nutzen zu können. Maßnahmen zur IT-Sicherheit sind eine rechtliche Pflicht, der sich die Verantwortlichen bewusst sein müssen. Wer etwa zur Verarbeitung von personenbezogenen Daten noch Windows XP mit seinen bekannten Mängeln nutzt, geht hohe Risiken ein, nicht nur Opfer von Datenklau zu werden, sondern muss sich auch darauf einstellen, eine empfindliche Strafe wegen eines Verstoßes gegen das DS-GVO begleichen zu müssen.

Die DS-GVO verlangt, dass die eingesetzten Datenverarbeitungssysteme belastbar sind. Dies bedeutet, dass Maßnahmen zur Aufrechterhaltung der Datenverarbeitung zu treffen sind. Dazu gehört beispielsweise eine unterbrechungsfreie Stromversorgung, um Datenverlust durch Stromausfall vorzubeugen.

Wird neueste IT-Hard- und Software eingesetzt, so ist dies bereits die halbe Miete. Doch auch ein Berechtigungsmanagement gehört zum Sicherheitskonzept. Statt einer Gruppenkennung sollte stets eine individuelle Kennung vergeben werden, damit ausgeschlossen wird, dass Personen sie nicht betreffende Daten einsehen können. Nicht vergessen werden darf, dass diese Zugriffsrechte nach dem Ausscheiden aus dem Unternehmen wieder entzogen werden.

Damit Angriffe von außen erschwert werden, sollten E-Mails verschlüsselt, Webseiten mit SSL-Zertifikat genutzt und WLAN-Netze verschlüsselt werden. Auf private Geräte im dienstlichen Umfeld sollte grundsätzlich verzichtet werden. Beim Versenden von E-Mails ist zudem darauf zu achten, dass weitere Empfänger stets im BCC-Feld eingetragen werden, da Einträge im CC-Feld für jeden Empfänger sichtbar sind, was einen Verstoß gegen das DS-GVO darstellt und unter Umständen ein Bußgeld nach sich zieht.

Die Verbreitung von Schadcode hat in den letzten Jahren massiv zugenommen. Besonders Ransomware verbreitet sich stark. Derartige Software ist in der Lage, die Festplatte eines Computers zu verschlüsseln, die erst gegen die Zahlung eines Lösegelds wieder entschlüsselt wird. Eine mögliche Sicherheitsmaßnahme ist ein Back-up-Management oder die zentrale Datenspeicherung auf ein Netzwerklaufwerk. Zu beachten ist jedoch, dass Daten in der Cloud ebenso verschlüsselt werden können, wenn eine automatische Synchronisation zwischen PC und Cloud aktiv ist. Hilfreich ist auch, für den E-Mail-Verkehr einen eigenen PC einzusetzen, auf dem sich keine relevanten Daten befinden und der nach einer Verschlüsselung rasch zu ersetzen ist. Nicht vergessen werden darf, dass laut DS-GVO die Datenschutz-Aufsichtsbehörde zu informieren ist, wenn personenbezogenen Daten durch einen Hacker-Angriff betroffen sind.

Gebäude sichern

Um die Daten zu schützen, ist es darüber hinaus nötig, ausreichende Schutzmaßnahmen zu ergreifen, die es Unbefugten erschweren, sich Zutritt in die Geschäftsräume zu verschaffen. Es ist daher wesentlich, zu registrieren, wer im laufenden Betrieb das Gebäude beziehungsweise entsprechende Räumlichkeiten betritt. Hier sind Sensorchips als Türöffner eine Lösung. Auch Nebeneingänge, die etwa für Erholungspausen genutzt werden, sollten nicht dauerhaft unverschlossen und unbeobachtet sein.

Lücken im Datenschutz eines Unternehmens aufzuspüren, ist Sache eines Datenschutzbeauftragten. Ein Datenschutzbeauftragter ist zwingend vorgeschrieben, wenn in einem Unternehmen oder Verein mindestens zehn Personen, egal ob bezahlt oder unbezahlt, damit beschäftigt sind, personenbezogene Daten automatisiert zu verarbeiten. Aber auch wenn dies nicht der Fall ist, muss unter Umständen ein Datenschutzbeauftragter bestellt werden. Dies ist dann der Fall, wenn etwa Daten zur Gesundheit, politischen Meinung oder der Gewerkschaftszugehörigkeit gespeichert werden und die Speicherung solcher Daten eine Kerntätigkeit des Unternehmens oder Vereins ist.

Wenn beispielsweise zwölf, rein ehrenamtliche Mitarbeiter eines Vereins die Daten der Abteilungsmitglieder automatisiert verwalten, muss ebenso ein Datenschutzbeauftragter bestimmt werden, wie im Fall eines Arztes, der lediglich zwei Mitarbeiter beschäftigt, jedoch die Gesundheitsdaten seiner Kunden speichert, was zur Kerntätigkeit seines Wirkens gehört.

Externe Experten einbeziehen

Unternehmen, die trotz Verpflichtung personell nicht in der Lage sind, einen Datenschutzbeauftragten zu bestellen, können dazu einen externen Dienstleister beauftragen. Wichtig ist, die Ernennung eines Datenschutzbeauftragten schriftlich durchzuführen, damit jederzeit gegenüber der Aufsichtsbehörde nachgewiesen werden kann, dass tatsächlich ein Datenschutzbeauftragter benannt ist. Diese Mitteilung ist der Aufsichtsbehörde stets zukommen zu lassen. Nicht vergessen werden darf, dass trotz Datenschutzbeauftragen die Verantwortung zur Einhaltung der Datenschutzvorschriften bei der Geschäftsleitung beziehungsweise dem Vereinsvorstand bleibt.

Damit sich Betroffene ohne Umwege direkt an den Datenschutzbeauftragten wenden können, sieht die DS-GVO vor, dass dessen Kontaktdaten veröffentlicht werden müssen, was sinnvollerweise auf der Internetseite des Unternehmens oder Vereins erfolgen sollte. Darüber hinaus sind der Name und die Kontaktdaten des Verantwortlichen zu nennen. Zudem müssen Informationen gegeben werden, was mit den personenbezogenen Daten passiert und wie lange diese gespeichert werden. Nicht vergessen werden darf ein Hinweis auf das Recht auf Auskunft, Berichtigung und Löschung. Ebenso müssen Kunden darauf hingewiesen werden, dass sie eine Einwilligung zur Datenverarbeitung jederzeit grundlos widerrufen können. Auch ein Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde darf

nicht fehlen. Nicht selten werden diese Rechte wohl bei Verstößen gegen das Persönlichkeitsrecht in Anspruch genommen. Insbesondere Fotos, die im Internet kursieren, sind häufig Streitobjekte, deren Entfernung von Homepageseiten verlangt wird. Dabei ist es völlig egal, ob diese Personen zufällig ins Bild marschierten und unbeabsichtigt mit aufgenommen wurden. Die DS-GVO sagt klar, dass Fotos, die Personen abbilden, personenbezogene Daten enthalten und ohne Erlaubnis der Person nicht veröffentlicht werden dürfen.

Verpixeln reicht nicht

Selbst wenn kein Name der auf dem Bild sichtbaren Person zugeordnet ist, ist diese Person von denjenigen Personen zu identifizieren, die sie kennen. Das können Bekannte, Freunde, Nachbarn oder Kollegen sein. Eine Verpixelung beseitigt diesen Personenbezug nicht unbedingt, da der Betroffene zumindest für seine Familie trotzdem noch erkennbar ist. Dies genügt, um den Personenbezug herzustellen. Ob Kopfform, Ohren, Frisur oder Körperhaltung – abgebildete Personen sind von guten Bekannten leicht zu identifizieren, manchmal sogar an der Bekleidung oder den Schuhen.

Es macht übrigens keinen Unterschied, ob Fotos im Internet oder im Intranet Verwendung finden. Die Persönlichkeitsrechte müssen immer beachtet werden. Im Arbeitsleben sollten Einwilligungen daher stets schriftlich festgelegt werden. Dadurch soll verdeutlicht werden, dass die Einwilligung eines Arbeitnehmers zur Veröffentlichung eines Bildes unabhängig von seinen Verpflichtungen aus dem Arbeitsverhältnis erfolgt. Die Schriftform muss jedoch nicht immer gegeben sein. Im Privatleben können auch Einwilligungen wirksam sein, die lediglich mündlich gemacht wurden.

Übrigens sollten sich Unternehmen hüten, derartige Einwilligungsklauseln in die Arbeitsverträge mit aufzunehmen, da diese oft zu allgemein ausfallen, daher den Arbeitnehmer unangemessen benachteiligen und daher unwirksam sind. Eine Einwilligung muss daher stets individuell erfolgen. Um rechtliche Risiken auszuschließen, ist es zudem nötig, den Verwendungszweck der Bilder genau zu beschreiben.

Zudem ist darauf zu achten, ob die Person noch minderjährig ist. In diesem Fall ist die schriftliche Einwilligung der Sorgeberechtigten einzuholen. Darüber hinaus muss auch der Minderjährige selbst der Bildaufnahme zustimmen.

Wichtig ist zu wissen, dass ein allgemeiner Hinweis bei einer Veranstaltung – dass Fotos gemacht werden, die auf der Homepage veröffentlicht werden – keine individuelle Einwilligung ersetzt. Vielmehr kann eine Person Auskunft verlangen, ob er fotografiert wurde.

Ganz wichtig ist zu wissen, dass das Auskunftsrecht dazu verpflichtet, in jedem Fall eine Anfrage zu beantworten, auch wenn man keine Daten oder Bilder von der anfragenden Person besitzt. Sind Daten vorhanden, so müssen diese als schriftliche oder elektronische Zusammenfassung offengelegt werden. Diese Pflicht trifft sowohl auf Unternehmen, als auch auf Vereine zu. Bei der Übertragung der Daten müssen nur diejenigen Daten offengelegt werden, die die betroffene Person selbst übermittelt hat. Ausgenommen sind Daten, wie etwa Kaufvorlieben, Zahlungsverhalten oder Retourenquote.

Daten einer Person dürfen etwa für Marketingzwecke nicht mehr genutzt werden, wenn die betroffene Person dagegen Widerspruch einlegt. Es sind dazu keine Gründe vorzutragen. Zudem ist darauf zu achten, dass Personen in aller Regel einen Anspruch darauf haben, dass Menschen und nicht Computer darüber entscheiden, wie mit den persönlichen Daten umgegangen wird.

Rasch reagieren

Anfragen und Wünsche zu den eigenen Daten müssen nicht irgendwann, sondern zügig, spätestens innerhalb eines Monats beantwortet und umgesetzt werden. Wird dem nicht nachgekommen, so können sich die Betroffenen an die Aufsichtsbehörde wenden, die in aller Regel das Fehlverhalten sanktioniert. Der Grund, warum man seiner Verpflichtung nicht nachgekommen ist, ist zu diesem Zeitpunkt nachrangig.

Ob Verein oder Unternehmen, kommt es zu einer Verletzung des Schutzes personenbezogener Daten, so muss dies der Aufsichtsbehörde gemeldet werden. Darunter fallen beispielsweise Vernichtung, Veränderung oder unbefugte Offenlegung der Daten. Wird diese Meldung unterlassen, drohen erhebliche Bußgelder, sogar dann, wenn kein nachweisbare Schaden enstanden ist. Verantwortliche können sich nicht herausreden, von der Datenpanne nichts gewusst zu haben. Das Gesetz schreibt vor, dass Strukturen zu schaffen sind, die dazu führen, dass solche Meldungen automatisch zum Verantwortlichen vordringen und zudem dokumentiert werden.

Interessant ist, dass von einer Datenpanne betroffene Personen nicht zwingend zu benachrichtigen sind. Vielmehr kommt es darauf an, ob die Datenschutzverletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser Person zur Folge hat.

Ernste Folgen drohen

Verstöße gegen das DS-GVO können ernsthafte rechtliche Folgen nach sich ziehen. Im Extremfall sind Geldbußen bis zu 40 Millionen Euro möglich. Selbst kleine Unternehmen und Vereine müssen damit rechnen, bei Verstößen eine Strafe im vier- oder gar fünfstelligen Bereich berappen zu müssen. Schon „Kleinigkeiten“ können diese Strafen auslösen. Dazu gehört das Versenden von E-Mails mit offenem Verteiler, der Aushang von Krankheitslisten von Mitarbeitern am „Schwarzen Brett“ oder wiederholte Faxsendungen mit medizinischen Daten an falsche Empfänger. Interessanterweise wird es keine offiziellen Angaben geben, wie hoch die jeweiligen Bußgelder bei Verstößen ausfielen. Begründet wird dies mit der Einzigartigkeit jedes Falls.

Zu Strafe kommen dann noch Schadensersatzansprüche, die jede Person stellen kann, der ein materieller oder immaterieller Schaden durch die Datenschutzverletzung entstanden ist.

Doch damit nicht genug. Die Aufsichtsbehörden sind entsprechend der europarechtlichen Vorgaben völlig unabhängig. Sie werden weder von übergeordneten Behörden, noch von Parlamenten kontrolliert. Sie können verdachtsunabhängig und ohne richterlichen Durchsuchungsbefehl jederzeit und unangekündigt Datenschutzprüfungen vor Ort durchführen. Den Behördenmitarbeitern muss Zugang zum Computer gewährt werden, damit Sie diesen überprüfen können. Diese Überprüfung kann bereits durch eine Beschwerde eines unzufriedenen Beschäftigten, Kunden oder Vereinsmitglieds ausgelöst werden.

Es lohnt sich daher, sich mit der neuen DS-GVO intensiv zu beschäftigen, damit die große Gefahr, die von diesem Gesetz ausgeht, nicht zu einer Katastrophe für Firmen und Vereine wird.

www.efdat.de