Die größten Datenschutzverstöße 2020

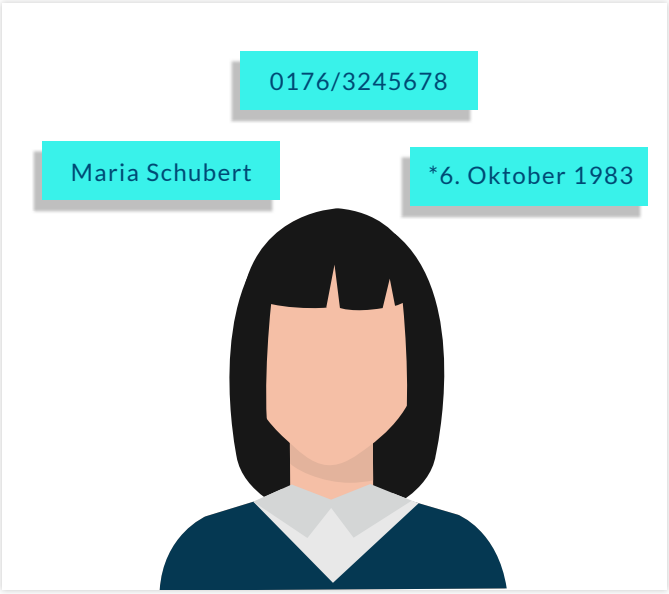
lawpilots

RECHT. EINFACH. VERSTEHEN.

Die größten Datenschutzverstöße 2020

Die 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) der Europäischen Union hat sich in den letzten Jahren als mächtiges Instrument erwiesen. Sogar internationale Tech-Konzerne wie Facebook, Google oder Microsoft passten ihren Umgang mit personenbezogenen Daten an die neue Verordnung an. Obwohl ihre heimischen Regulierungsbehörden sie diesbezüglich weniger einschränken.

Trotz alledem sind Datenschutzverstöße an der Tagesordnung, sei es durch die unrechtmäßige Erfassung von personenbezogenen Daten oder den fahrlässigen Umgang mit Datenschutzpannen. Auch die Auferlegung hoher Bußgelder, durch zuständige Datenschutzbeauftragte, geht durch die Einführung der DSGVO schneller vonstatten als noch vor einigen Jahren.



Was ist ein Datenschutzverstoß?

Als Datenschutzverstöße gelten alle Verstöße gegen die DSGVO. Ob es sich um eine Ordnungswidrigkeit oder Straftat handelt, hängt von der Schwere des Verstoßes ab. Viele Datenschutzverstöße gelten als Datenschutzverletzungen, weil eine „Verletzung des Schutzes personenbezogener Daten“ vorliegt.

Personenbezogene Daten beziehen sich auf Einzelangaben über persönliche oder sachliche Verhältnisse. Laut Art. 4 der DSGVO handelt es sich hierbei um alle Informationen, die sich auf eine reale natürliche Person beziehen. Die Weitergabe dieser Daten ist nur gestattet, wenn eine entsprechende Rechtsgrundlage, beispielsweise die Einwilligung der betroffenen Person vorliegt.

Die größten Datenschutzverstöße und -skandale 2020

H&M: Ausspähung von Mitarbeitenden

Die in Hamburg ansässige H&M Gesellschaft betreibt ein Service Center in Nürnberg, welches seit 2014 umfangreich die privaten Lebensumstände seiner Mitarbeitenden erfasst hat. Bis zu 50 Führungskräfte hatten Zugriff auf die abgespeicherten und teilweise aufgezeichneten Erkenntnisse zu Urlaubs- und Krankheitstagen. Dabei handelte es sich sowohl um die Speicherung von Krankheitssymptomen und Diagnosen sowie um private Informationen über familiäre Probleme oder religiöse Bekenntnisse.

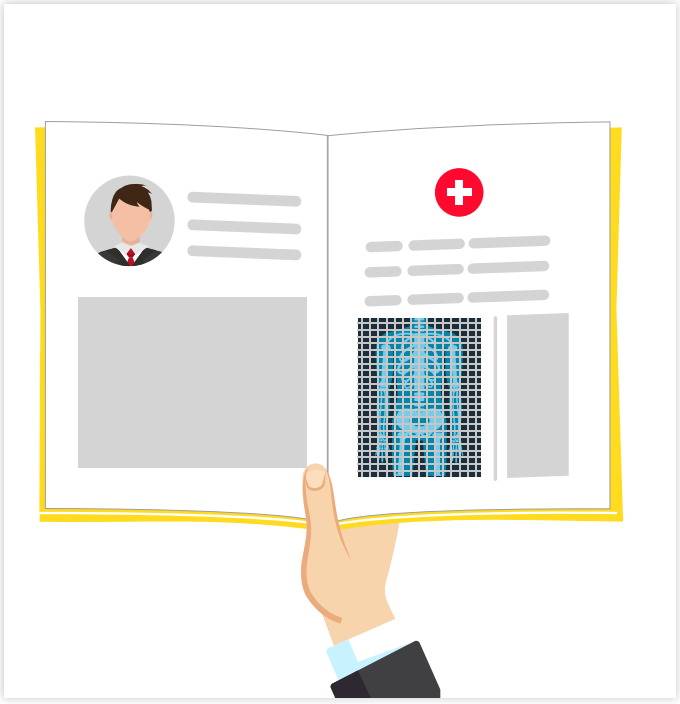
Aus den gesammelten Erkenntnissen und der Auswertung der Arbeitsleistung wurden Profile der Beschäftigten angelegt. Auf deren Basis die Führungskräfte Maßnahmen und Entscheidungen zum jeweiligen Arbeitsverhältnis trafen.

Das Vorgehen von H&M entspricht einer Verletzung des Art. 6 Abs. 1 DSGVO, da die betroffenen Personen keinerlei Kenntnis über die Aufzeichnung und Sammlung ihrer personenbezogenen Daten hatten.

Der Vorfall wurde bereits im Oktober 2019 bekannt, nachdem ein Konfigurationsfehler für mehrere Stunden allen Mitarbeitenden des Unternehmens die gesammelten Notizen zugänglich machte.

Der Hamburgische Beauftragte für Datenschutz stellte daraufhin das Netzlaufwerk mit einem Datensatz von ca. 60 Gigabyte sicher und vernahm zahlreiche Zeugen, deren Aussagen die Praktiken des Service Centers bestätigten.

Mittlerweile hat H&M ein neues Datenschutzkonzept ausgearbeitet und sich ohne Widerspruch dazu bereit erklärt dem Bußgeldbescheid von 35 Millionen Euro Folge zu leisten.



1&1: Unzureichende Sicherheit bei der Verarbeitung personenbezogener Daten

Der Mobilfunkanbieter 1&1 hingegen legte im letzten Jahr erfolgreich Widerspruch gegen einen Bußgeldbescheid des Bundesbeauftragten für Datenschutz und Informationsfreiheit ein.

Jener warf dem Unternehmen unzureichende Sicherheit bei der Verarbeitung personenbezogener Daten vor. Aufgefallen war dies durch einen Anruf bei der 1&1 Hotline.

Eine Frau hatte mit der bloßen Nennung des Namens und Geburtsdatums ihres Ex-Mannes dessen aktuelle Handynummer herausbekommen.

Der Bundesdatenschutzbeauftrage erkannte darin ein unzureichendes Authentifizierungssverfahren und legte für diesen Verstoß nach Art. 32 DSGVO ein Bußgeld von 9,5 Millionen Euro fest. Das Landgericht Bonn kürzte es nach Eingang des Widerspruchs aufgrund von Unverhältnismäßigkeit auf 900.000 Euro.

CapitalOne: Hackerangriff aufgrund von fehlender Cybersicherheit

Auf internationaler Ebene wurde in einem der größten Datenschutzskandale der letzten Jahre 2020 ein Bußgeld von 80 Millionen US-Dollar festgesetzt. Dem Finanzdienstleister Capital One wird vorgeworfen, dass das Unternehmen über unzureichend angemessene Cybersicherheitsprotokolle verfüge. Die US-amerikanische Behörde OCC führte dies auf ein Versäumnis aus dem Jahr 2015 zurück, indem Capital One ohne die Einrichtung entsprechender Risikobewertungsverfahren damit begonnen hatte Cloud-Speichertechnologie einzusetzen.

Auf das Datenleck waren die Behörden im Juli 2019 aufmerksam geworden, nachdem eine ehemalige Amazon-Mitarbeiterin sich in einen der Cloud-Server des Finanzdienstleisters gehackt hatte. Im Zuge des Angriffs stahl sie über 100 Millionen persönliche Kundendaten inklusive Sozialversicherungsnummern, Bank- und Kreditkarteninformationen.

EasyJet: Hackerangriff

Ein ähnliches Muster weist der Fall der britischen Fluggesellschaft EasyJet auf.

Im Januar 2020 konnten Hacker aufgrund eines Datenlecks, persönliche Daten und Informationen von über neun Millionen Kund:innen erbeuten. Neben Reisedaten wurden auch Bank- und mehr als 2000 Kreditkarteninformationen gestohlen.

Die britische Datenschutzbehörde ICO ermittelt seither, wie es zu der Datenschutzpanne kommen konnte und wer hierfür die Verantwortung zu tragen hat. Sollte sich herausstellen, dass unzureichende Security-Maßnahmen den Hacker Angriff erleichterten, könnte dies zu hohen Strafzahlungen für die Fluggesellschaft führen.

Buchbinder: Ungewollte Veröffentlichung von Kundendaten

Auch im Fall des deutschen Autovermieters Buchbinder kam es Anfang 2020 zu einem Datenskandal von dem mehr als drei Millionen Kund:innen betroffen waren.

Aufgrund eines Konfigurationsfehlers befand sich ein Server-Backup der kompletten Kundendatenbank des Autovermieters über einige Wochen öffentlich zugänglich im Internet. Betroffen waren unter anderem über 2,5 Millionen deutsche und 400.000 österreichische Kund:innen. Darunter auch zahlreiche Prominente, Politiker:innen und Diplomat:innen, deren private Kontaktdaten in der Datenbank verzeichnet waren.

Es ist unklar wie viele unbefugte Zugriffe es bereits auf die Datenbank gegeben hatte, bevor das Datenleck bemerkt wurde. Inwieweit den betroffenen Kund:innen Gefahr in Form von möglichen Betrugsmaschen oder Phishing-Attacken droht ist deshalb noch unklar.

Bislang sind auch noch keine Strafen bekannt, die Buchbinder im Sinne der Verletzung des Art. 6 DSGVO in Bezug auf die unrechtmäßige Verarbeitung von personenbezogenen Daten zu erwarten hat.

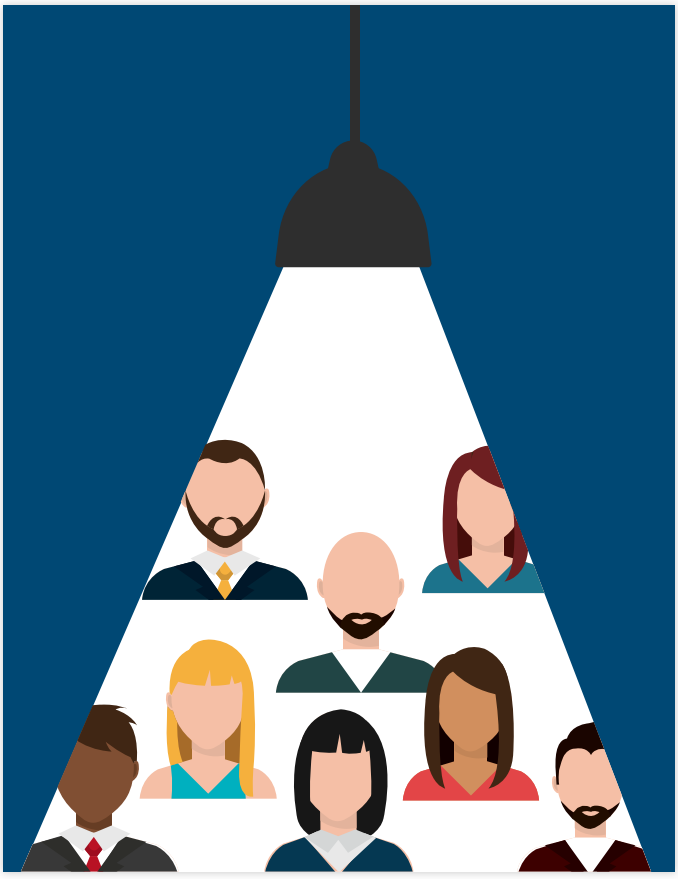
Carrefour France: Unzählige DSGVO-Verstöße

Im November 2020 kam es zu einem Urteil im Falle des Datenschutzskandals der in Frankreich ansässigen Carrefour Gruppe. Seit 2019 wurde hier im Hinblick auf mehrere Verstöße hinsichtlich der DSGVO ermittelt. Die französische Supermarktkette hatte u.a. die Daten von über 28 Millionen Teilnehmenden ihres Treueprogramms bis zu zehn Jahre lang aufbewahrt. Die zuständige Datenschutzbehörde CNIL hält in diesem Zusammenhang lediglich drei Jahre Aufbewahrungszeit für angemessen.

Auch Kopien von Personalausweisen und Identitätsnachweisen von Betroffenen wurden bis zu sechs Jahre vom Unternehmen aufbewahrt. Dabei hätten laut CNIL die Kopien sofort nach der Prüfung der Identität gelöscht werden müssen.

Ein Verstoß nach Art. 12 und 13 DSGVO wurde ebenfalls auf Grund von fehlender Transparenz in den Formulierungen der Datenschutzhinweise der Supermarktkette festgestellt. So waren die entsprechenden Richtlinien teilweise mehrdeutig oder ungenau formuliert und die Verarbeitung personenbezogener Daten wurde verallgemeinert oder lediglich beispielhaft dargestellt.

Die offiziellen Verstöße gegen Art. 5 DSGVO (und acht weitere Paragraphen der Datenschutz-Grundverordnung) führten am 18.11.2020 zu der Festlegung eines von Carrefour zu zahlendem Bußgeld von 2,25 Millionen Euro.



Österreich: „Der größte Datenschutzskandal der Republik“

Zu guter Letzt gab es 2020 auch einen Datenskandal, der über eine Million Österreicher betraf. Die Daten des sog. Ergänzungsregisters für Betroffene waren öffentlich einsehbar. Jenes war besonders in Zusammenhang mit der Coronakrise und dem Einrichten der Härtefonds hoch frequentiert. Das Register umfasst Daten von Kleinunternehmern und Selbstständigen, darunter auch Personen des öffentlichen Lebens. Neben der Nennung des Namens waren ihre Adressen und Geburtsdaten verzeichnet sowie in manchen Fällen weitere Angaben zum Beihilfebezug hinterlegt.

Auch hier waren die Daten von überall aus der Welt abrufbar und damit leichte Beute für den kriminellen Datenhandel.

Nach bekanntwerden des Skandals wurde das Register vom Netz genommen und eine Taskforce eingerichtet. Sie soll sich zukünftig für eine Lösung unter Berücksichtigung von Transparenz und Datenschutz einsetzen.

Würden Ihre Mitarbeitenden potenzielle Datenlecks rechtzeitig erkennen?

Viele Unternehmen würden bereits aus moralischer Überzeugung davon absehen ihre Mitarbeitenden „auszuspionieren“. Die neue Schlagkraft der Datenschutzbeauftragten rückt die Sicherheit der Mitarbeitenden- und Kundendaten jedoch für viele Unternehmen noch stärker in den Fokus.

Eine der Fragen, die es sich jetzt zu stellen gilt, ist:
„Wie sicher sind persönliche Daten in Ihrem Unternehmen?“

Dies hängt einerseits stark von den Security-Maßnahmen, andererseits von dem Bewusstsein der eigenen Beschäftigten ab. Eine generelle Awareness sowie Kenntnisse für den Umgang mit schützenswerten Daten erhöhen maßgeblich die Sicherheit ihres Unternehmens. Sie wirken präventiv und lassen Ihre Mitarbeitenden potenzielle Datenlecks rechtzeitig erkennen.

Neben nachgewiesenen Datenschutzverstößen und laufenden Untersuchungen standen 2020 auch einige digitale Anwendungen für ihren fragwürdigen Umgang mit Kundendaten in der Kritik.

Wie sicher sind unsere beliebtesten Kommunikations-Tools?

Zoom: Zoombombing und die Weitergabe an Dritte

Während der Coronapandemie und dem vermehrten Arbeiten auf Distanz stieg vor allem der Einsatz digitaler Informations- und Kommunikationstechnologie. Ein klarer Gewinner der Krise ist Zoom, ein amerikanischer Anbieter im Bereich der Videosoftware. Bereits die Visits von zoom.us stiegen von ca. 100 Millionen im Februar 2020 auf bis zu 1,9 Milliarden im April 2020 an.

Dann geriet der Videodienst jedoch zunehmend in die Kritik. Es sammelten sich Beschwerden über das plötzliche Auftauchen von pornografischen Inhalten oder Hassbotschaften in Videokonferenzen.

Auch das sog. „Zoombombing“, bei dem sich Fremde in ungeschützte Telekonferenzen einwählten und Schimpfwörter riefen oder Nazisymbole zeigten, mehrte sich.

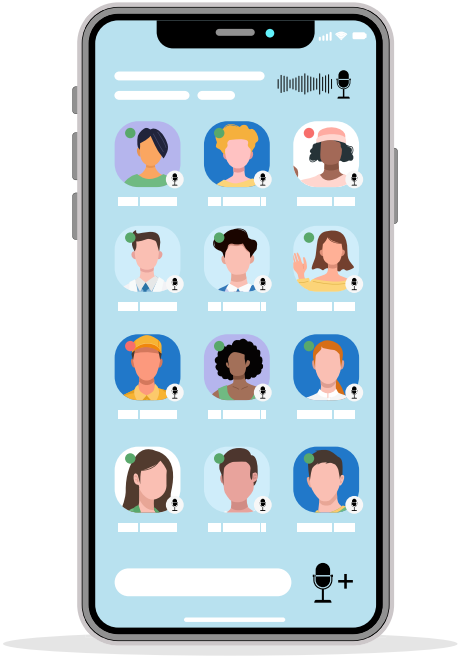
Diese Vorkommnisse waren besonders heikel, weil der Dienst während der Pandemie vermehrt von Krankenhäusern, Unternehmen, Universitäten und Schulen zur internen Kommunikation und im Rahmen des Homeschooling eingesetzt wurde.

Bereits im Frühjahr 2020 erfolgten Datenschutzuntersuchungen, da die iOS-App des Dienstes Informationen in Bezug auf verwendete Geräte, Speicherplatz und Bildschirmgröße an Facebook weitergegeben haben soll.

Auch die Möglichkeit der Überwachung von Videokonferenzen löste in Europa eine starke Datenschutzdebatte aus. Veranstaltende können sich mithilfe der Funktion anzeigen lassen, ob die Teilnehmenden während der Übertragung an ihrem Bildschirm anderen Aktivitäten nachgehen.

Mittlerweile hat Zoom auf viele der Kritikpunkte reagiert und aktiv mit den Aufsichtsbehörden zusammengearbeitet:

- Es wurde ein Warteraum für den kontrollierten Eintritt zu Videokonferenzen geschaffen
- Die Verwendung der Nutzerdaten zu wirtschaftlichen Zwecken wird jetzt ausdrücklich ausgeschlossen
- Videokonferenzen werden bereits seit Ende des Jahres 2020 in der kostenpflichtigen Version mit einer Ende-zu-Ende-Verschlüsselung versehen



Clubhouse: Verpflichtende Weitergabe der eigenen Kontakte

Ähnlich großes Skandalpotential scheint die seit Ende 2020 auch in Deutschland verfügbare Clubhouse-App zu haben. Sie stellt einen sog. „drop-in-audio-chat" dar, der vor allem für Live-Podcasts, denen bis zu 5000 Nutzern beitreten können, genutzt wird.

Eine Voraussetzung zur Nutzung der Anwendung ist die Freigabe des persönlichen Telefonbuchs. Die Server, auf denen die Kontaktdaten und Gespräche gespeichert werden, befinden sich in den USA. Dies hat zur Folge, dass Daten ohne die Zustimmung der betroffenen Person, übertragen und zu Werbezwecken o.ä. eingesetzt werden können.

Die Anwendung wird seit einigen Monaten in Europa und Deutschland angeboten. Und obwohl es von der DSGVO vorgesehen wird, verfügt Clubhouse über keine Datenschutzerklärung auf deutsch.

Des Weiteren gibt es weder ein Impressum noch eine Adresse für generelle Datenschutzauskünfte innerhalb der EU.

Daten richtig schützen

Der Wert der Daten steigt und damit auch das Risiko der unrechtmäßigen Weitergabe oder gezielten Cyber-Attacken. Diese Gefahren und die vermehrte Ahndung von Datenschutzvergehen führen zu höheren Ansprüchen an den Umgang mit personenbezogenen Daten im Unternehmen. Ebenso wie eine gewisse Wachsamkeit in Bezug auf die Datensicherheit bei populären Anwendungen wie Whatsapp, Facebook und Co.

Der größte Schutz vor Datenschutzskandalen und -verstößen ist und bleibt deshalb die Prävention. Eine Prävention die stark vom Wissen und Bewusstsein Ihrer Mitarbeitenden und Kolleginnen abhängig ist.

Denn Datenschutz beginnt sowohl bei der Person, die ihre eigenen Daten weitergibt, als auch bei jener die sie verarbeitet.

Dabei schützt nichts stärker vor unverhofften Pannen, als eine aufmerksame und geschulte Belegschaft. Mit unseren lawpilots Online-Schulungen, verfügbar in mehr als 30 Sprachen, stärken Sie Ihr Unternehmen, Ihre Organisation oder öffentliche Einrichtung im Bereich des Datenschutzes. Auf diese Weise fördern Sie das Vertrauen in Ihr Unternehmen, motivieren und bestärken Ihre eigenen Mitarbeitenden und verhindern die Entstehung möglicher Datenschutzvergehen.

Quellenverzeichnis

BBC (2020): EasyJet admits data of nine million hacked. 19.05.2020. Abgerufen am 24.01.2021. Verfügbar unter https://www.bbc.com/news/technology-52722626

c't (2020). Vorsicht, Chef liest mit! Heft 26/2020, S. 170-173

DSGV+O-Portal (2021). Geldbußen für DSGVO-Verstöße. Abgerufen am 25.01.2021. Verfügbar unter https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php

Flitter, E (2020), Capital One will pay $80 million over hack. Abgerufen am 25.01.2021. Verfügbar unter https://www.nytimes.com/2020/08/06/business/capital-one-hack-settlement.html

Handelsblatt (2021). Auf die Gerichte kommt es an. Ausgabe 19.01.2021, Seite 14.

LfDI Baden-Württemberg (2020). Pressemitteilung Zoom bessert nach. Abgerufen am 25.01.2021. Verfügbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/06/PM-Zoom-bessert-nach_fin.pdf

Spiegel Online (2020). Privatadressen von Promis und Politikern standen offen zugänglich im Netz. Abgerufen am 25.01.2021. Verfügbar unter https://www.spiegel.de/netzwelt/oesterreich-privatadressen-von-promis-und-politikern-standen-offen-zugaenglich-im-netz-a-fa1fa64d-c8a3-43d5-992d-475dd5516758

Statista (2020). Anzahl der Visits von zoom.us von Oktober bis 2019 bis September 2020. Abgerufen am 25.01.2020. Verfügbar unter https://de.statista.com/statistik/daten/studie/1113081/umfrage/anzahl-der-visits-pro-monat-von-zoom/

ZEIT ONLINE (2020). Vorwürfe gegen Zoom wegen mangelndem Datenschutz. Abgerufen am 25.01.2021. Verfügbar unter https://www.zeit.de/digital/datenschutz/2020-04/videodienst-zoom-datenschutz-hacker-angriffe-videokonferenzen?utm_referrer=https%3A%2F%2Fwww.google.com

JETZT EINFACH & KOSTENLOS TEST-VERSION
MIT DEM STICHWORT „E-LEARNING" ANFORDERN
UND UNVERBINDLICH BERATUNG VEREINBAREN.

www.lawpilots.com

lawpilots GmbH
Am Hamburger Bahnhof 3
10557 Berlin

+49 (0)30 22 18 22 80
kontakt@lawpilots.com

lawpilots

RECHT. EINFACH. VERSTEHEN.