Informationen Ihrer Datenschutzbeauftragten

IHRE DATENSCHUTZBEAUFTRAGTEN

Update September 2018

Sehr geehrte Leser,

der Juli, aber vor allem der August war der Monat der Betroffenenanfragen. Viele haben ihre Auszeit in den Ferien und das schöne Wetter dazu genutzt, sich mit den - durch die DSGVO erhaltenen - Rechten zu befassen. Für Verantwortliche bedeutet dies in der Regel: Erfüllung der Auskunftspflicht und die Bearbeitung von Löschbegehren. Mehr dazu im Newsletter!

Wir wünschen viel Spaß beim Lesen unserer Informationen und sind auf Ihre Rückfragen gespannt.

Haben Sie Fragen zu den hier beschriebenen Themen, oder dürfen wir Sie zu anderen Themen beratend zur Seite stehen? Nehmen Sie bitte Kontakt mit uns auf!

Freundliche Grüße

Ihre Datenschutzbeauftragten der CompliPro GmbH

INHALTSVERZEICHNIS

Auditfragebögen – erstes Update: Sie sind da! 3
Umgang mit Bewerbungsunterlagen 3
Japan – ein sicheres Drittland? 3
DSGVO und das Internetsterben… 4
Informationspflichten – Licht am Ende des Tunnels 4
E-Mail-Verschlüsselung – Pflicht durch die DSGVO? 6
Der Monat der Betroffenenrechte 6

AUDITFRAGEBÖGEN – ERSTES UPDATE: SIE SIND DA!

Wie in unserer August-Information bereits angemerkt, haben wir angefangen unsere Formulare in dynamischer und digitaler Form aufzubereiten. Die ersten Fragebögen stehen nun bereit und werden von uns anlassbezogen verwendet. Nachdem die Weiterentwicklung unserer ersten Schulungsplattform leider eingestellt wurde, mussten wir eine neue Lösung eruieren und glauben nun fündig geworden zu sein. Damit rücken die Mitarbeitersensibilisierungen in digitaler Form ebenfalls ein gutes Stück näher. Wir bleiben am Ball!

UMGANG MIT BEWERBUNGSUNTERLAGEN

Bereits zuvor haben wir darauf hingewiesen, dass die Bewerbungsunterlagen nach Abschluss des Bewerbungsverfahrens zu löschen sind. Der Erfa-Kreis der GDD in Würzburg hatte nun eine interessante Frage an die Aufsichtsbehörde:

Wenn Bewerbungen über eine Leih-/Zeitarbeitsfirma kommen, sind diese dann als Geschäftsbrief zu betrachten? Und unterliegen diese dann dadurch den entsprechenden Aufbewahrungspflichten? Muss dann hier unterschieden werden, ob der Kandidat eingestellt wurde, oder nicht?

Auf diesen Sachverhalt hat das BayLDA (Landesamt für Datenschutz in Bayern) wie folgt reagiert:

Wir sehen Bewerbungsunterlagen nicht als Geschäftsbriefe an, sodass die entsprechenden Aufbewahrungsvorschriften der Abgabenordung nicht einschlägig sind.

Bei abgelehnten Bewerbern kann der Arbeitgeber die Bewerbungsunterlagen daher – im Hinblick auf etwaige Ansprüche wegen Diskriminierung nach dem AGG – bis zu sechs Monate vorhalten, um in der Lage zu sein, die Berechtigung solcher Ansprüche zu überprüfen; anschließend sind die Unterlagen zu löschen bzw. zu vernichten. Wenn ein Bewerber eingestellt wird, werden seine Bewerbungsunterlagen Bestandteil der Personalakte und sind mindestens während seiner Betriebszugehörigkeit dort vorzuhalten.

Im Kern bedeutet dies, dass die Aufbewahrung von Bewerbungen sich nicht darin unterscheidet, ob die Bewerbung direkt oder über eine Zeitarbeitsfirma ins Unternehmen gelangt ist.

JAPAN – EIN SICHERES DRITTLAND?

Am 17.07.2018 haben die EU und Japan Ihre Verhandlungen erfolgreich abgeschlossen. Beide Seiten werden die Datenschutzsysteme auf beiden Seiten als „gleichwertig“ anerkennen, womit Japan in die Reihe der von der EU als sicher anerkannten Drittländer aufgenommen wird. Damit wird der Datentransfer zwischen der EU und Japan deutlich erleichtert. Seitens der EU müssen zum Abschluss noch der Europäische Datenschutzausschuss und ein Ausschuss aus Vertretern der Mitgliedsstaaten zustimmen, damit die Einigung wirksam wird.

IHRE DATENSCHUTZBEAUFTRAGTEN

DSGVO UND DAS INTERNETSTERBEN…

Mit Wirksamkeit der DSGVO wurden viele Webseiten und Blogs geschlossen. Teilweise aus Angst, teilweise weil man sich nicht vorbereitet hat und teilweise auch einfach, weil die Umsetzung der Vorgaben der DSGVO für das Projekt nicht mehr als wirtschaftlich betrachtet worden ist.

3 Monate sind nun vergangen – sind die Webseiten wieder online? Wir wissen es nicht.

Welche Webseiten zwischenzeitlich wieder zurückgekehrt sind und wie viele Webseiten endgültig offline gegangen sind ist uns leider unbekannt. Gerade für den deutschsprachigen Raum haben wir keine brauchbare Quelle gefunden. Ein Beispiel ist uns jedoch bekannt: pflegewiki.de [1]

VerifiedJoseph.com[2] führt jedoch eine Liste mit über 1.000 Webseiten, die immer noch auf Grund der DSGVO offline sind. Eine interessante Liste, die jedoch leider nur US-Webseiten enthält und daher für unseren Einzugsbereich nicht repräsentativ ist.

Auch nächstes Jahr könnte das Webseitensterben weitergehen – wir warten gespannt auf die neuen Regelungen, die uns die e-Privacy-Verordnung bringen wird. Der Entwurf bietet zumindest derzeit ausreichend Konfliktpotenzial!

INFORMATIONSPFLICHTEN – LICHT AM ENDE DES TUNNELS

Anfang des Jahres haben die Aufsichtsbehörden noch darauf bestanden, dass die Information des Betroffenen zum Zeitpunkt der Datenerhebung erfolgen muss und ein Medienbruch dabei nicht zulässig sei. Dreh- und Angelpunkt war immer die Formulierung „zum Zeitpunkt der Erhebung“ im Artikel 13 DSGVO[3].

Auch wenn die Aufsichtsbehörden immer noch nicht zu 100% den gleichen Weg eingeschlagen haben, sind die Aufsichtsbehörden doch langsam von dieser aus unserer Sicht weltfremden Auffassung abgewichen. Hier nochmal unsere Meinung zum Thema als kurze Zusammenfassung:

Ein Betroffener ruft an, muss ich am Telefon informieren?

Nein! Zumindest nicht, wenn die Datenverarbeitung dem entspricht, was der Betroffene nach dem Grundsatz „Treu und Glauben“ erwarten kann. Werden also die Daten im Rahmen einer telefonischen Terminvereinbarung für die Terminreservierung verwendet und keine anderen Zwecke verfolgt, so kann davon ausgegangen werden, dass dies genau der Verarbeitungsumfang ist, womit der Betroffene regelmäßig rechnen wird.

1 https://de.wikipedia.org/wiki/Pflegewiki
2 https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr
3 https://dsgvo-gesetz.de/art-13-dsgvo/

IHRE DATENSCHUTZBEAUFTRAGTEN

Und wenn ich nun eine Visitenkarte erhalte? Muss ich dann meine Informationen aushändigen?

Nein! Abgesehen davon, dass man die Datenschutzinformationen in solchen Fällen selten griffbereit hat, kann auch hier von den vom Betroffenen zu erwartenden Verarbeitungen ausgegangen werden. Im Rahmen Ihrer unternehmerischen Tätigkeit haben Sie ein berechtigtes Interesse an der Bewahrung von Geschäftskontakten und es ist nicht zu vermuten, dass der Betroffene dies nicht erwarten kann.

Muss ich dann überhaupt noch informieren?

JA! Immer dann, wenn erstmalig personenbezogene Daten vom Betroffenen erhoben werden. Allerdings sehen die europäischen Aufsichtsbehörden die Sache etwas lockerer als ihre deutschen Kollegen. Nach Meinung der europäischen Aufsichtsbehörden habe heute jeder Betroffene die Möglichkeit auf das Internet zuzugreifen. Damit erfüllen alle Verantwortlichen, die eine Datenschutzinformation auf der eigenen Webseite bereitstellen, die Informationspflichten der DSGVO.

Dann muss nur die Webseite angepasst werden und ich bin fertig?

Jein! Ganz so einfach ist es dann doch nicht. Online und am Telefon wird die Informationspflicht damit kein Problem mehr sein. Im Offline-Bereich wird es immer wieder Situationen geben, wo vielleicht Daten erhoben werden, jedoch noch keine Information stattgefunden hat. Und im Falle eines Ladenlokals oder einer Praxis wird man den Betroffenen nicht unbedingt auf die Webseite verweisen können.

Wie kann ich Offline in ausreichender Form informieren?

Hier empfiehlt sich ein gestufter Informationsprozess! Sorgen Sie dafür, dass die Basisinformationen und die notwendigen Informationen zur aktuellen Verarbeitung (z.B. „Fotos von Veranstaltungen“) vor Ort durch einen Aushang oder durch einen Flyer erfüllt werden. Verweisen Sie „für aller weiteren Details“ auf Ihre Datenschutzerklärung auf der Webseite.

Auch bei Geschäftsbriefen genügen die Datenschutzinformationen auf der Webseite. Stellen Sie den Link, ggf. auch als QR-Code, zur Verfügung.

Da es nicht immer der Fall sein wird, dass Sie erstmalig von einem Betroffenen kontaktiert werden, sondern ggf. selbst die Initiative ergreifen: Sorgen Sie mit einem Link in der E-Mail-Signatur auch hier für eine ausreichende Information des Betroffenen.

Unser Fazit:

Es wäre schön, wenn die Aufsichtsbehörden von Anfang an eine einheitliche und praktikable Art der Informationserfüllung genannt hätten. Leider ist dies bis heute nicht der Fall. Die „Guidelines on transparency under Regulation 2016/679“, wie die Meinung der europäischen Aufsichtsbehörden etwas sperrig heißt, helfen aber bei der Argumentation und Erfüllung der Informationspflichten.

IHRE DATENSCHUTZBEAUFTRAGTEN

E-MAIL-VERSCHLÜSSELUNG – PFLICHT DURCH DIE DSGVO?

Einige Softwarehersteller haben die DSGVO für sich entdeckt und argumentieren seit dem 25.05.2018 mit der DSGVO, um ihre Produkte zur E-Mail-Verschlüsselung zu vermarkten. Dabei wird gerne argumentiert, dass die DSGVO die Verschlüsselung der E-Mails zur Pflicht machen würde.

Ist dies tatsächlich so?

Die DSGVO sieht in der Tat die Verschlüsselung als Maßnahme zum Schutz personenbezogener Daten vor. Da die zu ergreifenden Maßnahmen jedoch unter Berücksichtigung von Schutzbedarf und Verhältnismäßigkeit umgesetzt werden müssen, kann nicht direkt von einer Pflicht zur Verschlüsselung ausgegangen werden.

Dazu die Aufsichtsbehörden:

„Übermittelt der Absender personenbezogene Daten mit normalem Schutzbedarf, besteht die Möglichkeit, im Einzelfall auf eine Ende-zu-Ende-Verschlüsselung der Inhaltsdaten zu verzichten. Als Mindeststandard ist bei der Übermittlung personenbezogener Daten mit normalem Schutzbedarf eine Transportverschlüsselung erforderlich.“

Umgekehrt bedeutet dies aber auch: Wenn von einem hohen Schutzbedarf ausgegangen werden kann, also Daten nach Art. 9 Abs. 1 DSGVO (Gesundheit, Religion usw.) übermittelt werden sollen, kann eine E-Mail-Verschlüsselung ggf. als notwendige Maßnahme betrachtet werden.

Sollten Sie Fragen zur E-Mail-Verschlüsselung oder zum Schutzbedarf Ihrer Daten haben, helfen wir Ihnen natürlich gerne weiter!

DER MONAT DER BETROFFENENRECHTE

Wie schon angesprochen, war der Juli und der August unsere Monate der Betroffenenrechte.

Außerdem kam uns noch der „DSGVO Horrorbrief“ oder der „Heise Horrorbrief“ auf den Tisch.
Dazu später mehr.

Die Menschen in der EU haben die DSGVO dazu genutzt aufzuräumen, die Flut der ungewünschten Newsletter hat aufgehört, nämlich eben jene die sich auf eine Einwilligung berufen haben und den Nachweis der Einwilligung nicht erbringen können. Das hat in vielen Postfächern für eine radikale „Newsletter-Diät“ gesorgt.
Ebenso konnten wir feststellen, dass wir einen massiven Anstieg der Betroffenenanfragen haben. Viele Menschen möchten einfach nur, dass Ihre Daten nicht mehr für Werbezwecke genutzt werden, es gibt viele Löschbegehren und auch viele **Missbrauchsversuche**.

Wir raten bei ausnahmslos jeder Betroffenenanfrage dazu, den DSB mit ins Boot zu holen um Fehler zu vermeiden, wie das Herausgeben von Informationen über Datensätze, die nach geltendem Recht

bereits gelöscht sein sollten. Diese Information kann der Betroffene ganz schnell gegen das Unternehmen des Verantwortlichen richten und damit bei der Aufsichtsbehörde an die Türe klopfen. Selbige kümmern sich derzeit übrigens gefühlt **nur** noch um Beschwerden von betroffenen Personen und nicht mehr um die Anfragen der Verantwortlichen, aber dazu mehr im nächsten Newsletter.

Ein weiterer auftretender Risikoaspekt der aufkommenden Auskunftsersuchen und Löschbegehren: Anfragen von Personen, die die Identifizierung ihrer Person verweigern. Eine Auskunft in solchen Situationen ist riskant, auch deshalb raten wir zur Konsultation des DSB sobald eine Betroffenenanfrage bei Ihnen eingeht. Teilweise ergehen diese Anfragen derzeit durch Dritte ohne entsprechende Vollmacht oder Rechtsgrundlage.
Wer hier eine Auskunft an einen fremden Dritten herausgibt, begeht eine Datenschutzverletzung und muss die Meldepflicht in 72 Stunden an die Aufsichtsbehörde einhalten. Wir als zertifizierte (Whitehat)-Hacker kennen solche Angriffe; Stichwort: Social Engineering!

Fazit: Sprechen Sie bitte mit uns BEVOR Sie eine Auskunft erteilen und denken an die Regelfrist von 4 Wochen für die Beantwortung von Betroffenenanfragen.

Was hat es jetzt mit diesem DSGVO Horrorbrief [4] auf sich?
Den Ursprung hat dieses Schreiben in Kanada. Viele wissen es gar nicht: Kanada ist datenschutzrechtlich ganz weit vorne mit dabei! Da wundert es nicht, dass ein Datenschützer in diesem Land einen Brief verfasst hat welcher ausnahmslos alle Register der DSGVO zieht und dem ungeübten Leser ganz schnell das Blut in den Adern gefrieren lässt, wenn er der Verantwortliche für die Datenverarbeitung ist. Constantine Karbaliotis hat das Schreiben verfasst und Roman Abashin hat ihn ins Deutsche übersetzt. Unter anderem wurde dieses Schreiben vom Heise-Verlag aufgegriffen und bekannt gemacht. Der eine oder andere nutzt diesen Brief jetzt um diversen Unternehmen gehörig auf den Keks zu gehen, mit Erfolg.

Kurz gesprochen: Sollten Sie diesen Brief mal auf den Tisch bekommen, raten wir zu folgendem Vorgehen: Weiterleiten an den DSB – wir wissen was zu tun ist!
Dieses Werk mit seinen vielfältigen Forderungen des Betroffenen haben wir für Sie bereits inhaltlich geprüft. Auch hier kann bei falscher Auskunft ein Datenschutzvorfall die Folge sein. Auf Grund der Detailtiefe der Fragen muss auch die Identifikation des Antragsstellers zu 101% schlüssig sein. Zudem sind einige Fragen zwar gegenüber der Aufsichtsbehörden zu beantworten, jedoch nicht gegenüber dem Betroffenen. Daher ist bei einigen Fragen ein Auskunftsanspruch zu verneinen, weil die DSGVO dem Betroffenen diese **nicht** zugesteht. Gut vorbereitet ist das Schreiben dann doch gar kein Horror mehr.

Wir helfen Ihnen gerne!

4 https://www.linkedin.com/pulse/nightmare-letter-subject-access-request-under-gdpr-karbaliotis/