Sehr geehrte Damen und Herren!

Anbei erhalten Sie unseren exklusiven Digital Solutions Infoletter mit wesentlichen Inhalten über aktuelle Entwicklungen und Neuigkeiten in den herausfordernden Bereichen DSGVO, e-privacy und NIS.

Selbstverständlich haben Sie die Option, diesen jederzeit mittels formlosen E-Mail an den Absender abzumelden.

1. „Was ist los mit der E-Privacy – Verordnung; Da war doch was?“

   Die E-Privacy-Verordnung (kurz ePVO) war ursprünglich als Ergänzung zu Regelungen der Datenschutz-Grundverordnung (DSGVO) gedacht. Ziel der ePVO ist es, europaweit die Vertraulichkeit in der elektronischen Kommunikation sicherzustellen, wobei sich die Regelungen dieser Norm auch auf nicht personenbezogene Daten im Online-Bereich beziehen.

   Aktueller Stand:

   Der ursprüngliche Termin für das Inkrafttreten der ePVO wäre 25.05.2018 gewesen, also zeitgleich mit der DSGVO. Die finale Fassung konnte allerdings bis heute nicht fertiggestellt werden. Angesichts der noch immer bestehenden Unstimmigkeiten zwischen den Mitgliedsstaaten ist es bisher nicht gelungen, einen gemeinsamen Standpunkt zum Verordnungsentwurf zu erzielen. Der deutsche Bundesverband für Digitale Wirtschaft (BVDW) rechnet daher vorsichtig mit einem Inkrafttreten nicht vor 2022.

   Wo gilt die E-Privacy-Verordnung?

   Der sachliche Anwendungsbereich erstreckt sich auf die Verarbeitung elektronischer Kommunikationsdaten, die in Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgt, und darüber hinaus auf Informationen in Bezug auf Endeinrichtungen der Endnutzer. Im Gegensatz zur DSGVO fällt auch die Verarbeitung nicht personenbezogener Kommunikationsdaten in den sachlichen Anwendungsbereich der ePVO.
   Räumlich gilt die Verordnung für die Bereitstellung elektronischer Kommunikationsdienste für Endnutzer in der Union sowie für die Nutzung solcher Dienste und den Schutz von Informationen in Bezug auf Endeinrichtungen der Endnutzer in der Union. Ist der Betreiber eines elektronischen Kommunikationsdienstes nicht in der Union niedergelassen, so muss er schriftlich einen Vertreter in der Union benennen.

   Für wen gilt die E-Privacy Verordnung?

   Adressaten der ePVO sind Betreiber elektronischer Kommunikationsnetze und -dienste, sohin eine Vielzahl von Unternehmen, die vielfältige Internetdienste, Kommunikationsplattformen und Onlinemarketing anbieten, auch aus Drittländern.

Konkreter sind darunter „Over-the-Top“ Dienste umfasst, wie zB Messenger, Web-Mailer oder Soziale Medien, aber auch die Kommunikation zwischen „smarten“ Geräten in der „IoT“ Umgebung.

Grundprinzipien der E-Privacy Verordnung

Elektronische Kommunikationsdaten sind vertraulich. Eingriffe in elektronische Kommunikationsdaten wie Mithören, Abhören, Speichern, Beobachten, Scannen oder andere Arten des Abfangens oder Überwachens oder Verarbeitens elektronischer Kommunikationsdaten durch andere Personen als die Endnutzer sind untersagt, sofern sie nicht durch die Ausnahmebestimmungen in der ePVO selbst erlaubt werden. Weiters enthält die ePVO genaue Regeln zur Speicherung und Löschung elektronischer Kommunikationsdaten. Bemerkenswert sind die Regelungen zum Schutz vor Datenerhebung aus den Endeinrichtungen der Endnutzer. Verpflichtend werden Einstellungsmöglichkeiten zum Schutz der Privatsphäre verlangt (privacy by design and by default).

Was droht bei Verstößen?

Die drohenden Geldbußen sind empfindlich hoch: Unzulässige Verarbeitung wird mit einer Strafe von bis zu EUR 10 Mio. oder bis zu 2% des gesamten weltweiten Jahresumsatzes eines Unternehmens sanktioniert, je nachdem welcher der beiden Beträge höher ist. Unzulässige Direktwerbung steht unter derselben Strafdrohung. Strafen von bis zu EUR 20 Mio oder von bis zu 4% des gesamten weltweiten Jahresumsatzes eines Unternehmens drohen bei Verstößen gegen den Grundsatz der Vertraulichkeit der Kommunikation, die erlaubte Verarbeitung elektronischer Kommunikation oder gegen die Nichteinhaltung der Löschfristen.
Darüber hinaus können Endnutzer materiellen oder immateriellen Schadenersatz geltend machen.
Einzigartig ist der Schutz von Geschäftsinteressen Dritter, indem ein ausdrückliches Klagerecht für Mitbewerber vorgesehen wird, sobald ein Betreiber elektronischer Kommunikationsdienste gegen die ePVO verstoßen hat.

Fazit

Auch wenn sich der Zeitpunkt des Inkrafttretens der ePVO gegen 2022 verschoben hat, sollten die Anforderungen der Verordnung rechtzeitig geprüft und mit dem aktuellen organisatorischen, rechtlichen und technischen Stand des Unternehmens verglichen werden. Ein umfassender Maßnahmenplan ist für die betroffenen Unternehmen unerlässlich. Die VACE Digital Solutions bietet Ihnen profunde und maßgeschneiderte Anleitung sowie Support durch berufserfahrene Experten, IT-Spezialisten, Juristen und Unternehmensberater.

Mag. Anna Tanyeli, MBA, 26. Februar 2020

2. “Löschkonzept”

Die DSGVO – Datenschutz-Grundverordnung, welche seit 25. Mai 2018 gilt – schreibt u.a. vor, dass personenbezogene Daten in solcher Form gespeichert werden, dass die Identifizierung Betroffener nur so lange möglich ist, wie es für den jeweiligen Verarbeitungszweck erforderlich ist (Art 5 Abs 1 lit e DSGVO).

Überhaupt haben Betroffene ein Recht auf Löschung bzw “Vergessenwerden”, welches mit Ausnahmen in Art 17 DSGVO geregelt ist. Wesentliche Ausnahmen – welche einer sofortigen Löschung entgegenstehen – sind zB “Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen” sowie Verarbeitung “zur Erfüllung einer rechtlichen Verpflichtung” .

Zum Beispiel: Ist der Verarbeitungszweck, zB Personalbewerbungen, welche nicht in einem Dienstvertrag münden, erfüllt – sind die personenbezogenen Daten nicht weiter vonnöten und müssen grundsätzlich gelöscht werden.

Ausgenommen: Kommt es wegen Verletzung des Gleichbehandlungsgebotes zu keinem Arbeitsverhältnis normiert § 26 Gleichbehandlungsgesetz eine Schadenersatzpflicht des “Arbeitgebers”. § 29 leg cit legt als Frist zur gerichtlichen Geltendmachung 6 Monate fest.

Laut Rechtsprechung muss ein konkreter Anspruch in einem konkreten Zeitraum befürchtet werden – hier könnte die Einhaltung des Gleichbehandlungsgebotes ohne entsprechende Unterlagen nicht dargetan werden; Weiters muss ein konkreter Zeitpunkt zur Löschung bestimmt sein.

Bis zur eigentlichen Löschung wird ein weiterer Monat Aufbewahrung der personenbezogenen Daten toleriert – dieser berücksichtigt den Fall einer späten Klagsführung innerhalb der Frist, welche dem Beklagten erst nach Ablauf der 6 Monate zur Kenntnis gelangt.
Im Ergebnis ist ein Aufheben von Bewerberdaten – sofern kein Dienstvertrag zustande kommt – bei entsprechender Dokumentation für 6 bis 7 Monate statthaft und muss im Anschluss gelöscht werden.

Nun geht Ihr Unternehmen nicht bloß mit Bewerberdaten um sondern sind 50 und mehr Verarbeitungstätigkeiten nach unserer Erfahrung keine Seltenheit. Dazu kommt, dass – um beim Beispiel der Bewerber als Betroffene zu bleiben – sich diese bekanntlich nicht in 6-Monats-Zyklen melden.

Innerhalb Ihres Unternehmens sind mehrere Stellen (HR, Fachabteilungsleiter, Geschäftsführer) mit der personellen Entscheidungsfindung befasst und kommen auch verschiedene EDV-Programme zum Einsatz – bedenken Sie den Fluss der personenbezogenen Daten.

Wird dem Bewerber schließlich ein Fahrtkostenersatz gegeben, ist eine Adress-Aufbewahrung "zur Erfüllung einer rechtlichen Verpflichtung" geboten - Empfängerbenennung zur Betriebsausgabe (§ 162 BAO) und 7 Jahre Aufbewahrungspflicht (§ 132 BAO).

Nur ein Löschkonzept, welches sich an der einschlägigen DIN (deutsche Norm) orientieren sollte, kann diesen Ansprüchen zur DSGVO-Compliance gerecht werden. Auch ist zur Umsetzung weitreichende Kenntnis der österreichischen und EU-Rechtsordnung gefragt.

Ein Löschkonzept regelt in der Zusammenschau mit Ihrem Verarbeitungsverzeichnis, welche personenbezogenen Daten an welche Stellen verteilt wurden, wo sich diese personenbezogenen Daten befinden und zu welchem Zeitpunkt diese gelöscht werden müssen:

- Welche Datenarten bilden eine Löschklasse?
- Welche Löschregeln gelangen zur Anwendung?
- Gibt es Ausnahmen?
- Wer ist zuständig?
- Wie wird dokumentiert?

Unsere konkreten Maßnahmenempfehlungen orientieren sich an anerkannten Standards (ISO, DIN) und ist mit höchster Wahrscheinlichkeit von behördlicher Anerkennung auszugehen.

Da die Löschpflicht aus einem Verarbeitungsgrundsatz (Art 5 DSGVO) sowie Betroffenenrecht (Art 17 DSGVO) erfließt drohen Unternehmen bei Verstößen Geldbußen von bis zu 20 Mio. EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist (Art 83 DSGVO).

Auch drohen dem Verantwortlichen Schadenersatzansprüche, sofern aus den Verstößen Personen Schäden entstehen - und vom Verantwortlichen kein Nachweis erfolgt, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Art 82 DSGVO).

In diesem Lichte ist dem Datenschutz insgesamt und speziell Ihrem Löschkonzept im Rahmen Ihres innerbetrieblichen Risikomanagements ein hoher Stellenwert zuzuschreiben.

VACE Digital Solutions bietet Ihnen in dieser Querschnittsmaterie aus IT-Security, Organisation und Recht die Errichtung und den Erhalt sowie kontinuierliche Verbesserung eines Datenschutz-Managementsystems durch berufserfahrene Juristen, Unternehmensberater sowie zertifizierte Datenschutzbeauftragte.

Mag. Christian Werbik, 12. Jänner 2020

3. “Berechtigtes Interesse”

Jede Verarbeitung von Personendaten ist auf – zumindest – einen Rechtsgrund zu stützen. Geht man von Personendaten aus, welche keine besonderen Kategorien darstellen, sind die Rechtsgründe nach Artikel 6 DSGVO wie folgt:

- Einwilligung
- (Vor-)Vertrag
- Rechtliche Verpflichtung des Verantwortlichen
- Lebenswichtige Interessen
- Öffentliches Interesse
- Berechtigtes Interesse des Verantwortlichen

Im Zusammenhang mit unternehmerischer Tätigkeit ist besonders das berechtigte Interesse relevant. An das berechtigte Interesse werden jedoch strenge Maßstäbe angelegt, was nicht selten zur Rechtsunsicherheit führt. Zunächst ist festzuhalten, dass es sich beim berechtigten Interesse nicht um einen Auffangtatbestand handelt – die sechs obenstehenden Rechtsgründe sind grundsätzlich gleichwertig. Bei der Prüfung eines berechtigten Interesses ist in drei Stufen vorzugehen:

Liegt ein berechtigtes Interesse des Verantwortlichen oder eines Dritten vor? Hier herrscht ein enger Zusammenhang mit dem Zweck der Verarbeitung und kommen wirtschaftliche, ideelle und rechtliche Erwägungen (Motive) in Frage. Berechtigt bedeutet in diesem Zusammenhang auch, dass das Interesse im Einklang mit der Rechtsordnung steht bzw nicht verboten ist.
Beispielsweise könnten Maßnahmen zur IT-Sicherheit, welche IP-Adressen speichern, ein berechtigtes Interesse sein – mit dem Zweck, Missbrauch und Betrug hintanzuhalten.

Für die Zulässigkeit einer Personendaten-Verarbeitung braucht es allerdings noch Erforderlichkeit und eine Interessenabwägung. Die Verarbeitung muss zur Wahrung des besagten Interesses erforderlich sein – geeignet, den Zweck zu erreichen. Damit geht einher, dass die Verarbeitung auf ein notwendiges Maß zu beschränken ist bzw darf kein gelinderes Mittel zur Verfügung stehen.

In einem dritten und letzten Schritt ist die Verarbeitung einer Abwägung mit Interessen, Grundrechten und Grundfreiheiten der betroffenen Person, “die den Schutz personenbezogener Daten erfordern”, zuzuführen. Dabei geht es nicht nur um ein Geheimhaltungsrecht für Personendaten sondern auch um freie Meinungsäußerung oder das Interesse, keine wirtschaftlichen Nachteile zu erleiden. Die Interessenabwägung berücksichtigt die Art und Weise der Verarbeitung sowie die konkreten Auswirkungen auf den Betroffenen. Sich gegenüberstehende Interessen sind zu gewichten; Verfassungsrechte oder der Allgemeinheit dienliche Betroffenen-Interessen werden besonders zu gewichten sein.

Mag. Christian Werbik, 1. März 2020

Mit freundlichen Grüßen
Ihr VACE Digital Solutions – Team

VACE Systemtechnik GmbH
Geschäftsstelle Steyregg
Linzer Straße 16e
A – 4221 Steyregg

Tel: +43 732 / 27 22 77 50
E-Mail: datenschutz@vace.at
Web: www.vace-sec.at

Digital Experts
IT-Services
IT-Security
Compliance

Details zu unseren Datenschutzbestimmungen finden Sie unter https://www.vace.at/de/datenschutz/

Dieser Infoletter stellt eine praxisnahe Einschätzung aktueller Schwerpunkte der Themen DSGVO, ePrivacy & NIS dar und erhebt keinen Anspruch auf Vollständigkeit. Keinesfalls kann der Newsletter als rechtssichere Empfehlungen angesehen werden.

Geschäftsleitung: Franz Humer, Klaus Kremmair, Andreas Obermüller
Firmenbuch Nr. FN 407593b . Landes- als Handelsgericht Linz, UID: ATU 68373306