Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 04/2022

Der IT-Ticker 04/2022 informiert Sie über folgende Themen:

- Datentransfer in die USA
- Google Fonts
- NIS 2-Richtlinie
- Cyber Resilience Act
- Datenschutz-Folgeabschätzung
- Ursachen Datenschutzverletzung
- Esport Recht

Keine Risiken mehr beim Datentransfer in die USA?

Der Datentransfer in die USA stellt nach wie vor ein schwieriges Thema für Betroffene und europäische Aufsichtsbehörden dar. Eine Datenübermittlung in die USA ist insbesondere aufgrund der weitreichenden Befugnisse von US Behörden mit großen Unsicherheiten verbunden und stößt Unternehmen vor große Herausforderungen.

Aktuell wächst jedoch die Hoffnung auf ein transatlantisches Datenschutzabkommen mit der EU. Am 7.Oktober 2022 unterzeichnete US Präsident Joe Biden eine neue Durchführungsverordnung, die sog. Executive Order „on Enhancing Safeguards for United States Signals Intelligence Activities“, welche einen neuen Rechtsrahmen zur Datenübermittlung in die USA schaffen soll und damit ein neues Kapitel zum Datentransfer in die USA eröffnet.

Executive Order

Bei der Executive Order handelt es sich um eine Verordnung der US-Regierung, welche für US-Behörden bindend ist. Diese sieht Regelungen vor, welche insbesondere die vom Europäischen Gerichtshof im sog. Schrems-II-Urteil vom 16. Juli 2020 (Rs. C 311/18) getroffenen Vorgaben umsetzen soll (vgl. unseren Webseitenbeitrag). Ziel dieser Verordnung soll es sein, eine rechtssichere Datenübermittlung zwischen den USA und der EU zu gewährleisten.

Konkret beinhaltet die Executive Order folgende Regelungen:

Zum einen sollen erstmals verbindliche Garantien zugesichert werden, welche die US-Geheimdienstaktivitäten auf ein bestimmtes Maß beschränken. Ein Zugriff auf die personenbezogenen Daten der EU Bürger soll hiernach nur dann möglich sein, wenn dies zur nationalen Sicherheit notwendig und die Beeinträchtigung verhältnismäßig ist. Zudem sollen verpflichtende Verfahren für US Geheimdienste eingerichtet werden, welche eine wirksame Überwachung der neuen Standards für den Schutz der Privatsphäre von EU Bürger gewährleisten. Darüber hinaus ist auch die Einführung eines Rechtsbehelfssystems vorgesehen, welches erstmalig EU-Bürgern eine unabhängige und verbindliche Überprüfung ihrer Rechte garantieren soll. Hierbei handelt es sich um ein zweistufiges Verfahren: Auf der ersten Stufe soll EU-Bürgern die Möglichkeit einer Beschwerde bei dem „Director of National Intelligence“ gegeben werden, welche auf einer zweiten Stufe durch das neu geschaffene unabhängige Datenschutzgericht, sog. „Data Protection Review Court", überprüft werden kann.

Zum Hintergrund

Die Executive Order beruht auf einer Grundsatzeinigung der EU-Kommission und der USA:
Nach langen Verhandlungen wurde in einer gemeinsamen Erklärung am 25.03.2022 verkündet, dass sich die EU und die USA auf ein neues Transatlantisches Datenschutzabkommen, das sog. Trans-Atlantic Data Privacy Framework (TADPF), geeinigt haben. Hiermit soll nach Auffassung der EU-Kommission eine dauerhafte Grundlage für den transatlantischen Datenverkehr geboten sowie die Rechte der Bürger geschützt werden.

Weitere Schritte

Nun ist die EU Kommission an der Reihe: Entscheidend für die Umsetzung dieser neuen Verordnung ist die Fassung eines Angemessenheitsbeschlusses seitens der EU Kommission, welcher festlegt, dass die USA ein der DS-GVO entsprechendes angemessenes Datenschutzniveau bieten. Bis es allerdings soweit ist, wird noch etwas Zeit vergehen. Mit dem Erlass kann nämlich voraussichtlich erst in sechs Monaten gerechnet werden. Rechtssicherheit bei der Datenübermittlung in die USA gibt es insofern erst, wenn ein solcher Angemessenheitsbeschluss vorliegt.
Bis dahin sollten Unternehmen weiterhin auf die Anwendung von Transfermechanismen, wie beispielsweise auf den Abschluss von Standardvertragsklauseln („SCC“) bzw. der Implementierung von Binding Corporate Rules („BCR“) achten sowie auf die Durchführung einer Risikobewertung, sog. Transfer Impact Assessment („TIA“). Die Executive Order kann allerdings im Rahmen der Risikobewertung als Verbesserung des Datenschutzniveaus in den USA herangezogen und mitberücksichtigt werden.

Ausblick

Vor diesem Hintergrund sollte unbedingt folgendes beachtet werden:
Ab dem 27. Dezember 2022 darf eine Datenübertragung in Drittländer ausschließlich auf Grundlage der – von der EU Kommission im Juni 2021 erlassenen - neuen Standardvertragsklauseln erfolgen. Nach Ablauf dieser Frist verlieren alle alten Klauseln ihre Wirksamkeit, weshalb im Falle ihrer Anwendung hohe Bußgelder und Schadenersatzforderungen drohen. Aus diesem Grund sollten Unternehmen dringend Ihre bestehenden Verträge dahingehend überprüfen, ob diese noch die alten Standardvertragsklauseln beinhalten. Sollte dies der Fall sein, empfehlen wir mit Blick auf den baldigen Fristablauf, die notwendigen Schritte einzuleiten und die alten Standardvertragsklauseln durch die Neuen EU-Standradvertragsklauseln zu ersetzen.

Insgesamt bleibt abzuwarten, ob das neue Transatlantische Abkommen dem europäischen Datenschutzniveau standhalten wird. Jedenfalls kann davon ausgegangen werden, dass das Transatlantische Abkommen früher oder später zur rechtlichen Überprüfung vor dem Europäischen Gerichtshof landen wird.

Marwah Kamal,
Franziska Ladiges,
Nikolaus Bertermann

Achtung bei Google Fonts: Datenschutzrechtliche Abmahnwelle

Es ist keine Neuigkeit, dass Datenschutzaufsichtsbehörden den Einsatz von Drittinhalten, die von Unternehmen wie Google kostenlos zur Einbindung auf Webseiten zur Verfügung gestellt werden, kritisch sehen. Ebenso ist stets das Thema der Datenübertragung in die USA zu berücksichtigen.

Seit kurzem haben sich nun allerdings auch einige Anwaltskanzleien speziell auf die Abmahnung des Einsatzes von nachgeladenen Schriften wie Google Fonts fokussiert. Hierbei werden zahlreiche vor allem kleinere und mittelständische Unternehmen wegen angeblich rechtswidrigen Einsatzes der genannten Schriften oder anderen Drittinhalten mit Verweis auf allgemeine Persönlichkeitsrechtsverletzungen abgemahnt. Hierbei wird sich vor allem auf die Entscheidung des LG München I, Endurteil vom 20.01.2022 – 3 O 17493/20 gestützt. Das Gericht hat hier entschieden, dass dem Kläger im konkret vorliegenden Einzelfall ein Anspruch auf Schadensersatz zusteht. Es hielt die Einbindung von Google Fonts ohne Einwilligung für rechtswidrig, da durch den Einsatz von Google

Fonts eine Übermittlung der IP-Adresse an Google Server in den USA erfolgte. In den jeweiligen Abmahnungen werden von den betroffenen Unternehmen nun Einmalzahlungen von 100-170 EUR gefordert.

Bei Google Fonts handelt es sich um ein Schriftenverzeichnis von mehr als 1000 Schriften, welche das amerikanische Unternehmen Google kostenfrei zur Verfügung stellt. Webseitenbetreiber können diese Schriften zur Darstellung ihrer Texte einbinden. Die Schriftarten können entweder lokal/on premises auf dem eigenen Server oder (und das ist der hier abgemahnte Weg) über die Google-Server gehostet werden.

Wir weisen darauf hin, dass sich einige der Abmahnungen neben dem Verweis auf die Schriftarten auch auf den Einsatz von Drittinhalten wie von Cloudflare ohne entsprechende Einwilligungserklärungen beziehen.

Wie finde ich (oder eine Abmahnkanzlei) heraus, ob meine Webseite Google Fonts und Co. einsetzt?

Auch wenn Sie (noch) keine Abmahnung erhalten haben, sollte einmal sorgfältig geprüft werden, welche Drittinhalte auf der Webseite des Unternehmens eingebunden sind. Die Inhalte und Drittverbindungen, die zu Servern - wie bspw. dem von Google - aufgebaut werden, lassen sich sehr einfach technisch feststellen. Sie können entweder durch Rechtsklick auf der gewünschten Webseite im Browser den Punkt „Seitenquellentext anzeigen“ auswählen. Finden sich dann im Quelltext Angaben wie „fonts.googleapis.com“ oder „fonts.gstatic.com“ sind die Schriften vermutlich über den Google Server eingebunden und ein Datentransfer zu Google findet statt. Alternativ können Sie sich auch über die „weiteren Werkzeuge“ im jeweiligen Browser die „Werkzeuge für Webentwickler“ anzeigen lassen. Auf diese Weise sehen Sie über die entsprechende „Netzwerkanalyse“ und den „Webspeicher“ weitere Details zu den jeweils eingebundenen Inhalten.

Achtung, teilweise verstecken sich Inhalte wie Google Fonts auch dann, wenn Sie andere Plugins auf der Webseite einbinden. Sind beispielsweise andere Google Inhalte wie Google Maps oder reCaptcha eingebunden, ist es ebenfalls möglich, dass Bestandteile von Google Fonts eingebunden werden.

Wie gehe ich vor, wenn ich auf der Webseite den Einsatz von Google Fonts, die über den Google Server gehostet werden, festgestellt habe?

Wie im letzten Schritt beschrieben, ist für jeden Dritten – also Abmahnkanzleien aber auch Datenschutzaufsichtsbehörden, die empfindliche Bußgelder verhängen können – einsehbar, welche Drittinhalte eingebunden sind. Hier sollten Sie sich also gar nicht erst potentiell angreifbar machen. Vor diesem Hintergrund ist von einem Einsatz von Google Fonts in der Version, in welchem ein Datentransfer auf einen Google Server stattfindet, dringend abzuraten. Es sollte entweder die Variante gewählt werden, in welchem die Google Fonts nach einem Download lediglich lokal eingebunden (hierzu finden sich online zahlreiche Anleitungen wie bspw. hier) oder gänzlich auf die Einbindung fremder Schriftarten verzichtet werden.

Was mache ich, wenn ich eine der genannten Abmahnungen erhalte?

Als erstes sollten Sie den Einsatz der Webfonts – sollte er überhaupt tatsächlich erfolgt sein – unterbinden. Von voreiligen Zahlungen der auf den ersten Blick gering erscheinenden Summen ist zudem abzuraten. Aus unserer Sicht kommt bei den Abmahnwellen ein rechtsmissbräuchliches Verhalten durch die Abmahnkanzleien in Betracht. Melden Sie sich gerne, wenn Sie entsprechende rechtliche Unterstützung bei dem Umgang mit den genannten Abmahnungen benötigen.

Helena Kasper,
Hannah Mugler,
Nikolaus Bertermann

Anforderungen an die IT-Sicherheit in Unternehmen - Die NIS 2-Richtlinie kommt

Mittlerweile täglich werden u.a. Betreiber kritischer Infrastruktur Opfer von Hackerangriffen bzw. Cyberattacken. Der deutsche Gesetzgeber reagierte bereits letztes Jahr mit der Verschärfung der

gesetzlichen Anforderungen an die von den Betreibern umzusetzende IT-Sicherheit durch das IT-Sicherheitsgesetz 2.0. Der europäische Gesetzgeber zieht nun nach und geht mit dem zuletzt von der EU-Kommission vorgeschlagenen Cyber Resilience Act für Produkte mit digitalen Elementen (CRA, wir berichteten) und der NIS 2-Richtlinie die nächsten Schritte seiner Cybersecurity-Strategie.

Die am 28.11.2022 verabschiedete Aktualisierung der Richtlinie über die Sicherheit von Netz- und Informationssystemen (kurz: NIS 2-Richtlinie) weitet u.a. den Geltungsbereich der aus dem Jahr 2016 stammenden NIS-Richtlinie aus. Danach sollen mehr Einrichtungen und Sektoren zu substanzielle(re)n Maßnahmen im Bereich der Cybersicherheit verpflichtet werden.

Mehr Unternehmen + mehr Pflichten = mehr IT-Sicherheit?

Neben den bisher von der NIS-Richtlinie abgedeckten kritischen Bereichen (Energie, Verkehr, Wasser, Gesundheit, digitale Infrastruktur und Finanzwesen) müssen nach entsprechender Umsetzung der Richtlinie u.a. auch Anbieter öffentlicher elektronischer Kommunikationsdienste und digitaler Dienste, Betreiber sozialer Medien, Hersteller kritischer Produkte (z. B. Medizinprodukte) sowie Post- und Kurierdienste ihre Maßnahmen im Bereich der IT-Sicherheit überprüfen und gegebenenfalls anpassen.

So werden auf die betroffenen Unternehmen und Betreiber u.a. folgende Risikomanagementmaßnahmen zukommen:

- Teilnahme der Leitungsorgane an Schulungen zum Thema Cybersicherheit und Durchführung solcher für die Mitarbeiter;
- Implementierung geeigneter und verhältnismäßiger technischer, operativer und organisatorischer Maßnahmen, die auf einem gefahrenübergreifenden Ansatz zu beruhen haben unter notwendiger Beachtung u.a. der Sicherheit der Lieferketten, den möglichen Einsatz von Kryptografie sowie Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Technologiesystemen;
- Einhaltung von strafferen Berichtspflichten für erhebliche Sicherheitsvorfälle: erste Meldung an die zuständige nationale Behörde innerhalb von 24 Stunden, innerhalb von 72 Stunden detaillierter Bericht, Abschlussbericht nach einem Monat;
- Registrierungs-/Auskunftspflichten gegenüber nationalen Behörden zur Erhebung und Führung von Übersichten von Betreibern kritischer Infrastruktur.

Bußgelder für die Unternehmen, Konsequenzen für Führungskräfte

Damit die umfassenden Sicherheitsanforderungen auch umgesetzt werden, erweitert der europäische Gesetzgeber die möglichen Aufsichtsmaßnahmen der nationalen Behörden (z.B. Vor-Ort-Kontrollen, regelmäßige Sicherheitsprüfungen einschließlich Ad-hoc-Prüfungen) und legt strengere Durchsetzungsvorschriften fest.

Bei Verstößen droht den Betreibern ein Bußgeld bis zu zehn Millionen EUR statt der in Deutschland bisher maximalen zwei Millionen EUR oder von mindestens 2% des gesamten weltweiten Umsatzes. Daneben können im Einzelfall erteilte Genehmigungen

für die von den Betreibern kritischer Infrastruktur erbrachter Dienste oder Tätigkeiten vorübergehend ausgesetzt und den Führungskräften direkt die Wahrnehmung der Leitungsaufgaben untersagt werden.

Warum nicht nur Betreiber der kritischen Infrastruktur betroffen sind

Ergänzend zur Erweiterung der Sektoren um Domain-Registrierungsstellen kommt auch die Pflicht, dass diese künftig die persönlichen Informationen aller Domain-Inhaber wie Name, Adresse und Telefonnummer speichern müssen. Auf Anfragen von Strafverfolgungsbehörden haben sie innerhalb von 72 Stunden zu antworten. Anonyme Dienste dürften es somit in Zukunft schwerer haben.

Und auch Unternehmen, die zunächst nicht der Qualifizierung als kritische Infrastruktur unterfallen, sollten die Umsetzung der Richtlinie im Blick behalten. Denn nicht nur können die Mitgliedsstaaten die Betreiber kritischer Infrastruktur verpflichten, bestimmte IT-Produkte und -Dienste zu verwenden. Für solche können sie auch eine Zertifizierungspflicht vorsehen. Welche Anforderungen die Hersteller

dieser Produkte und Dienste für eine erfolgreiche Zertifizierung erfüllen müssen, hängt von (gegebenenfalls neuen) sogenannten Schemas für die Cybersicherheitszertifizierung ab, die die Agentur der Europäischen Union für Cybersicherheit („ENISA“) im Auftrag der EU-Kommission erarbeitet und von letzterer unter Umständen für verpflichtend erklärt werden kann.

Und nun?

Nachdem der Rat dem Entwurf zuletzt zustimmte, wird die Richtlinie in den kommenden Tagen im Amtsblatt der Europäischen Union veröffentlicht und tritt am zwanzigsten Tag nach ihrer Veröffentlichung in Kraft. Danach haben die Mitgliedstaaten 21 Monate Zeit, die Richtlinie in nationales Recht umzusetzen.

Unternehmen sind aber auch schon jetzt gut beraten, ihre IT-Sicherheit kritisch zu überprüfen und gegebenenfalls weitere Schutzmaßnahmen umzusetzen. Angreifer warten ohnehin nicht auf regulatorische Eingriffe des Staates. Eine frühzeitige Überprüfung und Anpassung der unternehmenseigenen Sicherheit erleichtert zudem die Konformität mit den zu erwartenden nationalen Bestimmungen.

Allerdings dürfte insoweit ohnehin noch nicht das Ende der Fahnenstange erreicht sein. Denn angesichts der Zunahme der Bedrohungen und deren Auswirkungen auf die Wirtschaft und das gesellschaftliche Leben ist zu erwarten, dass weitere Anforderungen an die IT-Sicherheit gestellt und bestehende Vorgaben weiter verschärft werden. Die Mitgliedstaaten haben jedenfalls die Möglichkeit, bei der Umsetzung der NIS 2-Richtlinie über deren Vorgaben hinauszugehen und strengere Regeln aufzustellen, sofern nicht bereits (teilweise) geschehen. Gut, dass der deutsche Gesetzgeber derzeit parallel schon finanzielle Unterstützung für betroffene Unternehmen ins Spiel bringt.

Dr. Thomas Hohendorf

Vorschlag der EU-Kommission für einen „Cyber Resilience Act“

Am 15.9.2022 hat die EU-Kommission ihren Verordnungsvorschlag für einen Cyber Resilience Act („CRA“) veröffentlicht (2022/0272 (COD)). Der CRA enthält Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen. Die Umsetzung dieser Anforderungen soll durch Marktüberwachung und erhebliche Sanktionsdrohungen gewährleistet werden.

Der CRA ist Bestandteil der Cybersecurity Strategie der EU-Kommission. Ein weiterer Baustein der Cybersecurity Strategie ist etwa die als NIS2-Richtlinie bezeichnete Überarbeitung der bestehenden Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie). Weitere Informationen zur NIS2-Richtlinie finden Sie in Kürze auf unserer Webseite.

Die Vorgaben des CRA gelten für „Produkte mit digitalen Elementen“. Der Begriff umfasst dabei alle Software- und Hardware-Produkte sowie „remote“ Datenverarbeitungslösungen, ohne die eine vorgesehene Funktion des jeweiligen Produkts mit digitalen Elementen nicht ausgeführt werden könnte. Lediglich manche spezifisch regulierte Produkte sind vom Anwendungsbereich des CRA ausgenommen. Dieser Anwendungsbereich ist also denkbar breit angelegt. Einige wesentliche Vorgaben des CRA sind im Folgenden zusammengefasst.

1. Anforderungen an Produkte mit digitalen Elementen

Der CRA enthält allgemeine Marktzugangsregelungen für Produkte mit digitalen Elementen. Diese dürfen nur in Verkehr gebracht werden, wenn (1) das Produkt selbst grundlegende Anforderungen an die Cybersecurity erfüllt und (2) Anforderungen an Prozesse für den Umgang mit Schwachstellen der Cybersecurity erfüllt werden.

Für die Anforderungen an das Produkt und an die Prozesse für den Umgang mit Schwachstellen unterscheidet der CRA in drei Risikoklassen zwischen (1) „normalen“, (2) „kritischen“ und (3) „hochkritischen Produkten“ mit digitalen Elementen. Je nach Klassifizierung eines Produkts gelten unterschiedlich Anforderungen. Hersteller müssen allerdings stets eine Konformitätsbewertung für das jeweilige Produkt und die Prozesse durchführen. Konforme Produkte müssen eine ordnungsgemäße

CE-Kennzeichnung führen und dürfen nur mit einer solchen Kennzeichnung auf den Markt gebracht werden.

2. Anforderungen an Marktteilnehmer

Neben Konformitätsbewertung und CE-Kennzeichnung treffen Produktherstellerweitere Pflichten. Dazu gehört etwa der Umgang mit Schwachstellen, einschließlich der kostenlosen Bereitstellung von Security Updates. Diese Pflicht gilt für die gesamte Lebensdauer des Produkts, längstens jedoch für 5 Jahre ab erstem Inverkehrbringen in der EU. Zudem sind Hersteller verpflichtet, bestimmte Schwachstellen und Vorfälle mit Auswirkungen auf die Produktsicherheit an die ENISA zu melden und Nutzer über Sicherheitsvorfälle zu informieren.

Importeure müssen vor Inverkehrbringen von Produkten mit digitalen Elementen sicherstellen, dass der Hersteller eine ordnungsgemäße Konformitätsbewertung durchgeführt und die erforderliche technische Dokumentation erstellt hat sowie dass das Produkt über die CE-Kennzeichnung und die erforderlichen Informationen und Nutzungshinweise verfügt. Bei Kenntnis von oder Verdacht auf nicht vorhandene Konformität ist der Importeur zur Veranlassung von Abhilfemaßnahmen oder – wenn angemessen – zur Einstellung des Vertriebs oder zum Rückruf des Produkts verpflichtet. Erhebliche Cybersicherheitsrisiken muss der Importeur zudem an die Marktaufsicht melden.

Distributoren sind vor Vertrieb eines Produkts mit digitalen Elementen verpflichtet, sich von der ordnungsgemäßen CE-Kennzeichnung und der Erfüllung der Pflichten von Herstellern und Importeuren zu überzeugen. Bei Kenntnis von oder Verdacht auf nicht vorhandene Konformität treffen einen Distributor dieselben Pflichten wie einen Importeur.

3. Sanktionierung

Der CRA sieht für Verstöße erhebliche Ordnungsgelder vor. Diese betragen nach dem Verordnungsvorschlag für Hersteller bis zu 15 Mio. EUR oder 2,5 % des weltweiten Umsatzes im vorherigen Wirtschaftsjahr, für andere Verstöße bis zu 10 Mio. EUR oder 2 % dieses Jahresumsatzes. Machen Hersteller, Importeur oder Distributor gegenüber einer Konformitätsbewertungsstelle oder der Marktaufsicht unzutreffende, unvollständige oder irreführende Angaben, betragen die möglichen Bußgelder bis zu 5 Mio. EUR oder 1 % des Jahresumsatzes, wobei jeweils die höhere Zahl maßgeblich ist.

4. Einführungsfristen

Die Regelungen des CRA sollen 24 Monate nach seinem Inkrafttreten anwendbar werden, die Informationspflichten der Hersteller über ausgenutzte Schwachstellen und Sicherheitsvorfälle jedoch bereits nach 12 Monaten. Mit dem Vorschlag der EU-Kommission hat zunächst das Verfahren der EU für den Erlass des Cyber Resilience Act begonnen.

Dr. Damiel Meßmer,
Martin Schweinoch

How to „Datenschutz-Folgenabschätzung“

Ausnahmslos jedes Unternehmen, ob Mittelstand oder Großkonzern, muss sich regelmäßig die Frage stellen, wie eine wirksame Datenschutz-Compliance sichergestellt werden kann. Neben allgemein bekannten Begrifflichkeiten wie den Datenschutzhinweisen oder dem sog. Verarbeitungsverzeichnis, kann insbesondere die Datenschutz-Folgenabschätzung als ein wirksames Instrument zur umfassenden Bewertung eines bestimmten Datenverarbeitungsvorgangs angesehen werden.

Obgleich eine Vielzahl an Prozessen letztlich einer Datenschutz-Folgenabschätzung zu unterziehen ist, stoßen wir in unserer Beratungspraxis erstaunlich häufig auf Probleme, Fehlvorstellungen und Schwierigkeiten beim Umgang mit diesem Verfahren. Dies hängt mitunter damit zusammen, dass vielen Unternehmen nicht wirklich bewusst ist, welche Informationen eine Datenschutz-Folgenabschätzung tatsächlich abbilden muss. Zudem sollte darauf geachtet werden, dass die jeweiligen Ausführungen - trotz der technischen Komplexität einiger Verfahren - für den Leser (ggf.

auch die Aufsichtsbehörde) verständlich bleiben. Um Ihnen insoweit eine erste „Stütze“ zur Verfügung zu stellen, sollen die wichtigsten Aspekte nachfolgend aufgezeigt werden.

Die Fakten

Art. 35 Abs. 1 der Datenschutz-Grundverordnung (DS-GVO) sieht für bestimmte „Formen der Verarbeitung“, welche aufgrund der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, die Durchführung einer Datenschutz-Folgenabschätzung vor. Obgleich eine Risikobewertung stets anhand sämtlicher Umstände des Einzelfalls zu erfolgen hat, existieren einige Hilfestellungen, welche eine entsprechende Bewertung ermöglichen.

So sind zunächst in Art. 35 Abs. 3 DS-GVO verschiedene Fälle aufgelistet, in denen eine Datenschutz-Folgenabschätzung durchzuführen ist. Dies betrifft bspw. die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (klassisches Beispiel: Videoüberwachung). Wie sich dem Wortlaut der Norm entnehmen lässt („insbesondere“) sind die explizit aufgezählten Fälle nicht abschließend. Daneben existiert eine sog. „Muss-Liste“ (vgl. Art. 35 Abs. 4 DS-GVO), in welcher die Datenschutzaufsichtsbehörden verbindlich die Durchführung einer Datenschutz-Folgenabschätzung vorschreiben. Die in diesem Kontext erarbeiteten Fallgruppen wurden dabei nicht „willkürlich“ bestimmt, sondern auf Basis von einigen vordefinierten „Risikokriterien“ aus Working-Paper 248 der Art.-29-Datenschutzgruppe entwickelt. Hierzu gehört bspw. die Datenverarbeitung in einem großen Umfang sowie die Verarbeitung vertraulicher oder höchst persönlicher Daten. Je mehr der jeweiligen „Risikofaktoren“ vorliegen, desto eher sollte eine Datenschutz-Folgenabschätzung durchgeführt werden.

Letztlich handelt es sich bei den einschlägigen Konstellationen regelmäßig um solche Anwendungsfelder, welche bereits nach dem gesunden „Bauchgefühl“ zu einem entsprechenden (hohen) Risiko für betroffene Personen führen (können). So liegt es auf der Hand, dass bspw. biometrische Kontrollsysteme, Videoüberwachungsanlagen oder Krankenhausinformationssysteme mit der Durchführung einer Datenschutz-Folgenabschätzung verbunden sind.

Der Inhalt einer Datenschutz-Folgenabschätzung

Kommt eine verantwortliche Stelle also zu dem Ergebnis, dass eine Datenschutz-Folgenabschätzung durchzuführen ist, gibt Art. 35 Abs. 7 DS-GVO einige Punkte vor, welche zwingend abzubilden sind. Neben einer systematischen Beschreibung der geplanten Verarbeitungsvorgänge, müssen auch die dabei verfolgten Zwecke, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit sowie (als das „Herzstück“) eine Risikoanalyse nebst ergriffenen Abhilfemaßnahmen dargestellt werden.

Insbesondere die Sachverhaltsaufklärung und -darstellung ist dabei von zentraler Bedeutung. Die verantwortliche Stelle sollte insbesondere ermitteln, welche weiteren Beteiligten in den Datenverarbeitungsvorgang eingebunden sind (bspw. Auftragsverarbeiter), welchen „Lebenszyklus“ die jeweils betroffenen Daten durchlaufen, insbesondere welche Hard- und Softwarekomponenten (einschließlich weiterer Schnittstellen zu anderen Systemen) eingebunden werden, über welchen Zeitraum die Daten aufbewahrt werden und wer auf die Daten Zugriff hat, bzw. haben kann. Insbesondere vermeintlich „unwichtige“ Details, wie bspw. Support-Leistungen in Drittländern (bspw. im Falle von Remote-Zugriffen) können zu erheblichen datenschutzrechtlichen Risiken führen. Erst wenn u.a. die vorgenannten Umstände zweifelsfrei festgestellt wurden, kann beurteilt werden, welche Risiken bei dem jeweiligen Datenverarbeitungsvorgang real bestehen. Auch die Bestimmung einer datenschutzrechtlichen Rechtsgrundlage sowie die Bewertung, ob die Datenverarbeitung notwendig und verhältnismäßig ist, bedarf einer lückenlosen Sachverhaltsaufklärung.

Die Risikobewertung

Ein Risiko bemisst sich aus dem Verhältnis zwischen der Schwere eines (denkbaren) Schadens und dessen Eintrittswahrscheinlichkeit. Zur Bewertung der real bestehenden Risiken, kann sich ein Unternehmen insbesondere an der eigens hierfür geschaffenen Matrix der Datenschutzkonferenz in Kurzpapier Nr. 18 orientieren.

In dem angeführten Kurzpapier wird unter einem Risiko „das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann“, verstanden. Gemäß Erwägungsgrund 75 der DS-GVO sind hierbei psychische, materielle und immaterielle Schäden denkbar.

Zunächst muss daher maßgeblich auf die zu erwartenden Schadenspositionen abgestellt werden. Erwägungsgrund 85 der DS-GVO nennt dabei typische Fallgruppen: Verlust der Kontrolle über die eigenen Daten, Einschränkung von Rechten, Diskriminierung, Identitätsdiebstahl oder -betrug, Finanzielle Verluste, Aufhebung der Pseudonymisierung, Rufschädigung, Verletzung des Berufsgeheimnisses oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

Betrachtet man die einzelnen (nicht abschließenden) Schadenspositionen, so muss neben deren Schwere auch im Einzelfall überprüft werden, mit welcher Eintrittswahrscheinlichkeit insgesamt zu rechnen ist. In diesem Kontext muss insbesondere abgeklärt werden, welche denkbaren Ursachen existieren, die zu einem entsprechenden Schaden führen können. Hier gibt es eine Vielzahl denkbarer Fallkonstellationen, zu denen bspw. Hacking-Angriffe, der (interne) missbräuchliche Umgang mit den Daten oder Schwächen in der Systemqualität gehören können. Um eine effiziente Bewertung der Eintrittswahrscheinlichkeit zu ermöglichen, müssen zudem auch bereits ergriffene sowie vorgesehene technische und organisatorische Maßnahmen im Sinne des Art. 32 Abs. 1 DS-GVO berücksichtigt werden.

Schaut man sich die vorgenannten Kriterien gründlich an, so kommt man schnell zu dem Ergebnis, dass die Durchführung einer Datenschutz-Folgenabschätzung keine einfache Aufgabe darstellt und eine Vielzahl an Faktoren beachtet werden müssen. Andererseits muss jedoch ebenfalls berücksichtigt werden, dass das jeweilige Dokument nicht „überfrachtet“ wird und für den Leser verständlich bleibt.

Methodische Vorgehensweise als wirksame Stütze

Um an dieser Stelle etwas „Licht ins Dunkel“ zu bringen, können wir Sie zunächst beruhigen. Mit der richtigen Planung und Vorgehensweise lässt sich eine Datenschutz-Folgenabschätzung effizient durchführen. So haben wir auf Basis unserer Erfahrungen u.a. in der Automobilbranche sowie im Gesundheitssektor wirksame Methoden entwickelt, die der Aufklärung des maßgeblichen Sachverhalts dienen und hierbei die klassischen Fragestellungen berücksichtigen. Auch für die jeweiligen Rechtsfragen können wir auf eine Vielzahl an Muster-Dokumenten, Legal-Tech-Anwendungen und Erfahrungswerten zurückgreifen. Wird eine Datenschutz-Folgenabschätzung richtig geplant und im Anschluss effektiv durchgeführt, kann auch der eine oder andere Stolperstein in der Datenschutz-Compliance behoben und einer praktikablen Lösung zugeführt werden.

Marius Drabiniok

Häufige Ursachen von Datenschutzverletzungen und Abwehrmaßnahmen

Die Datenschutzaufsicht in Sachsen-Anhalt hat aktuell eine tabellarische Übersicht zu häufigen Datenschutzverletzungen mit entsprechenden Abwehrmaßnahmen veröffentlicht. Die Tabelle beruht auf konkreten Auswertungen von Datenschutzverletzungen, die im Bundesland Sachsen-Anhalt der dortigen Datenschutzaufsicht gemeldet wurden. Erfreulich ist, dass die Datenschutzaufsicht Sachsen-Anhalt zu jeder Datenschutzverletzung konkrete Abwehrmaßnahmen benennt, mit denen Verantwortliche den Datenschutzverstoß beheben können. Zudem werden Abwehrmaßnahmen konkret vorgeschlagen, wie derartige Datenschutzverletzungen in der Zukunft vermieden werden können.

Die von der Datenschutzaufsicht Sachsen-Anhalt veröffentlichte tabellarische Übersicht, die nicht datiert ist, hat einen Umfang von zwei Seiten.

Diese Übersicht ist hier abrufbar.

Das SKW Datenschutz- & Cyber Security-Team ist eines der größten Teams im Markt. Wir beraten seit vielen Jahren unsere Mandaten im Zusammenhang mit Cyber-Attacken und allen anderen meldepflichtigen Datenschutzverletzungen. Wir unterstützen jederzeit bei Datenschutzverletzungen mit unserem Know-how.

Dr. Oliver Hornung

Europäisches Parlament verabschiedet Resolution zu Esport und Gaming

Ein historischer Moment für den Esport in Europa: Europäisches Parlament verabschiedet Resolution zu Esport und Gaming

I. Der Beginn des Prozesses

Der Prozess des Europäischen Parlaments bzgl. Esport begann am 8. November 2021 mit dem „Report on EU sports policy: assessment and possible ways forward". Unter der Überschrift „Supporting the transition to a sustainable and innovative future" heißt es unter Punkt 92 „[The European Parliament] calls for the EU institutions to launch a debate on the future and on the opportunities of e-sports and to collect data in order to assess this sector and present a study on its social and economic impact".

II. Forschung als Grundlage für den Prozess

Für das Erstellen dieser Studie, welche die Grundlage für den Prozess in den nachfolgenden zwölf Monaten legen sollte, beauftragte das zuständige CULT Committee (Ausschuss für Kultur und Bildung) Dr. Tobias M. Scholz und mich. Darüber hinaus gab der Ausschuss auch eine „Policy Recommendation" bei uns in Auftrag. Zweck dieser Werke und der Beratung bis zur Abstimmung im Parlament war es, den politischen Prozess auf europäischer Ebene zu begleiten und insbesondere den „Draft Report on E-sport and videogames" (Rapporteur Laurence Farreng) vorzubereiten. Sowohl die "Background Analysis on Esports" als auch die "Policy Recommendation on Esports" wurden am 9. März 2022 eingereicht und – nach einer Q&A Session der Abgeordneten mit den Autoren am 14. März 2022 – im Mai 2022 veröffentlicht.

Die Studie beschreibt den Status quo des Esports sowie die Chancen und Herausforderungen, die sich aus dem Esport ergeben. Die Policy Recommendation legt einen Fokus auf die Definition, Forschung, Regulierung und den Nutzen von Esport für die europäische Gesellschaft. Der auf diesen Publikationen basierende Draft Report wurde nur wenige Tage zuvor veröffentlicht. Der Report schloss sich den Publikationen in einem Großteil der in diesen behandelten Punkte an, unter anderem bzgl. der:

- Kernelemente der Esport-Definition
- Implikationen im Hinblick auf Kultur, Medien, Technologie und (traditionellen) Sport
- Nutzung von Esport als Werkzeug für Bildung
- Trennung von Esport und (traditionellem) Sport bei gleichzeitigem Fokus auf möglicher Zusammenarbeit bzw. Ergänzung
- Kategorisierung des Esports als Digital- und Innovationsmaterie
- Erstellung einer europäischen Langzeitstrategie für Gaming und Esport
- Verortung von Rechtssetzung auf europäischer Ebene und der Schaffung eines tauglichen Rechtsrahmens in verschiedenen Bereichen

Am 17. Mai 2022 wurde der „Draft Report on E-sport and videogames" schließlich über 30 Minuten im CULT Committee diskutiert. Dabei skizzierte die Berichterstatterin Laurence Farreng ihre drei Ziele bei der Erstellung des Berichtsentwurfs:

- die Industrien Gaming und Esport voranzubringen und die kulturellen und wirtschaftlichen Potenziale zu nutzen
- zu definieren, welchen Beitrag die EU leisten kann
- Esport hervorzuheben und zu fördern (Wertschätzung von Esport, Abbau von Barrieren und Stärkung der europäischen Identität durch Esport)

III. Änderungs- und Ergänzungsphase

Zwischen Mai und Mitte Oktober 2022 wurden die 229 Änderungsanträge diskutiert und Kompromisse ausgearbeitet – eine stattliche, aber keine besorgniserregende Menge an Anträgen. Bis zur Abstimmung im CULT Committee am 3. Oktober 2022 konnte aber für sämtliche Punkte ein Kompromiss erreicht werden.

IV. Abstimmung im CULT Committee

Am 3. Oktober 2022 fand die Abstimmung über den finalen „Report on esports and video games" im CULT Committee des Europäischen Parlaments statt. Der Report wurde in dieser Sitzung einstimmig angenommen und in seiner finalen Form vom 13. Oktober für die Plenarsitzung des Parlaments vorbereitet.

V. Debatte im Europäischen Parlament

Am 9. November 2022 fand ab 22 Uhr MESZ die 30minütige Debatte im Europäischen Parlament statt. Sämtliche Redner (u.a. Rapporteur Laurence Farreng, EU-Kommissar für Binnenmarkt und Dienstleistungen Thierry Breton) bescheinigten dem Report ein durchweg positives Zeugnis. Besonders gelobt wurde der holistische Ansatz, der sich nicht nur in finanzieller Unterstützung erschöpft, sondern sämtliche kulturellen und gesellschaftlichen Nutzungsmöglichkeiten beleuchtet und regulatorisches Handeln verlangt. EU-Kommissar Breton versicherte zum Abschluss, dass die Kommission sehr glücklich mit dem Report ist und plant, entsprechend tätig zu werden (eventuell in Verbindung zur derzeit laufenden Debatte zum Bereich Metaverse).

VI. Abstimmung im Europäischen Parlament

Am 10. November 2022 um 11 Uhr MESZ wurde schließlich die Resolution vom Europäischen Parlament verabschiedet. Am Ende des 12-monatigen Prozesses steht somit ein historischer Meilensteil, der gleichzeitig aber auch erst den Anfang der wahren Arbeit markiert. In den folgenden Monaten gilt es für den europäischen Gesetzgeber nun, den Worten des Parlaments Taten folgen zu lassen, um eine gesunde und erfolgreiche Entwicklung des Esports in Europa zu unterstützen.

VII. Zum Abschluss: Einige Highlights aus der Resolution

- The European Parliament calls for the development of a coherent, long-term European video game strategy, which should benefit all actors involved fairly and adequately, while taking into account esports and the current dependence on imports and building on existing national strategies in order to support EU actors and EU start-ups in these sectors;
- The European Parliament believes that, owing to the borderless nature of the discipline, the European Union is the appropriate level at which to address the challenges of esports;
- The European Parliament asks the Commission to study the possibility of creating coherent and comprehensive guidelines regarding the status of professional esports players;
- The European Parliament calls on the Member States and the Commission to consider the creation of a visa for esports personnel based on the Schengen cultural and sports visas, applicable to all personnel involved in running and participating in esports competitions, and to consider measures to facilitate visa procedures to enable video game workers to come to the EU;
- whereas the innovative value of the sector should also be acknowledged, as much as its cultural added value;
- whereas these ecosystems still lack the harmonised data, definitions and legal frameworks required to enable them to embrace their full potential;
- whereas video games and esports use advanced technologies such as AI and virtual reality, and have initiated the creation of alternative virtual spaces such as metaverses;
- whereas the definition [of esports] encompasses a human element (the players), a digital element (the games themselves) and a competitive element;
- whereas esports differ from sports in that they are digital by definition; whereas esports is a phenomenon essentially driven by private entities, with the IP rights belonging to the game publisher and competition rights either to the game publisher or arranged on a contract-by-contract basis;

- The European Parliament considers that esports and sport are different sectors, not least because the video games used for competitive gaming or esports are played in a digital environment and belong to private entities that enjoy full legal control and all exclusive and unrestricted rights over the video games themselves; believes, however, that both sectors can complement and learn from each other and promote similar positive values and skills, such as fair play, non-discrimination, teamwork, leadership, solidarity, integrity, antiracism, social inclusion and gender equality;
- The European Parliament acknowledges the need to safeguard esports from problems with match-fixing, illegal gambling and performance enhancement, including doping; underlines the necessity to prevent doping and match-fixing in professional gaming and to educate players about these issues, as well as to protect the integrity of competitions;
- The European Parliament calls on the Commission to explore synergies between the video game sector and its innovation strategy, particularly in the context of research on the metaverse and bearing in mind the protection of data privacy and cybersecurity challenges, without losing sight of the esports phenomenon;
- The European Parliament calls on the Commission to develop a charter to promote European values in esports competitions, in partnership with publishers, team organisations, clubs and tournament organisers;
- The European Parliament underlines that video games and esports have a dual role to play in the green transition, both as an industry that must work to become more environmentally friendly, and as a medium for raising awareness of climate and environmental issues among video game players;
- The European Parliament highlights the important role that cities and regions can play in providing access to infrastructure capable of hosting esports events or facilitating access to video games for all

Dr. Nepomuk Nothelfer