ICDPPC

Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

ENTSCHLIESSUNG ZUR AUSEINANERSETZUNG MIT DER ROLLE DES MENSCHLICHEN IRRTUMS BEI VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

41. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

22. Oktober 2019, Tirana, Albanien

Sponsoren

- Office of the Australian Information Commissioner, Australien

CO-Sponsoren:

- Autoriteit Persoonsgevens, Niederlande;
- Comisssao Nacional de Protecçao de Dados, Portugal;
- Commission Nationale de l'Informatique et des Libertés, Frankreich;
- Data Protection Commission, Irland;
- Information Commissioner's Office, Vereinigtes Königreich;
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Mexiko;
- National Privacy Commission, The Philippines;
- Office of the Privacy Commissioner, Neuseeland;
- Office of the Privacy Commissioner of Canada, Kanada

Die 41. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre:

Unter HINWEIS DARAUF, dass zum Schutz der Privatsphäre natürlicher Personen und zur Stärkung des Vertrauens in die Datenwirtschaft eine globale Antwort der Datenschutzbehörden erforderlich ist, und zwar aufgrund der Zunahme der Anzahl, des Umfangs und der Schwere der Verletzungen des Schutzes personenbezogener Daten, ihrer gemeinsamen Ursachen, ihrer Folgen auf internationaler Ebene und des Schaden, der sich daraus ergeben kann,

In DEM BEWUSSTSEIN, dass die Einführung von Systemen zur Meldung von Verletzungen des

Schutzes personenbezogener Daten in einigen Mitgliedstaaten zu einer erheblichen Zunahme der Meldung von Verletzungen des Schutzes personenbezogener Daten führte und wertvolle Einblicke in ihre Ursachen erlaubte, und ein besseres Verständnis dafür ermöglicht hat, wie sie vermieden werden können, und dass mögliche Präventionsstrategien ermittelt werden können;

Unter HERVORHEBUNG, dass Meldungen über Verletzungen des Schutzes personenbezogener Daten und regulatorische Maßnahmen in einigen Rechtsprechungen der Mitgliedstaaten sowie nationale und internationale Studien belegen, dass bei Verletzungen des Schutzes personenbezogener Daten häufig ein menschlicher Irrtum vorliegt, insbesondere, dass Arbeitnehmer unbeabsichtigt personenbezogene Daten an unbefugte Empfänger weitergeben, oder dass sich Personen aufgrund eines Betrugs zur Preisgabe von Benutzeranmeldeinformationen verleiten lassen, was den Zugang zu Informationen und Systemen ermöglicht („menschlicher Irrtum“);

In der ERKENNTNIS, dass weltweit ein Grundsatz des Rechts auf Privatsphäre und Datenschutz darin besteht, dass personenbezogene Daten durch angemessene Sicherheitsvorkehrungen gegen Risiken wie Verlust, unbefugten Zugang, Vernichtung, Nutzung, Änderung oder Offenlegung geschützt werden sollten;

In BEKRÄFTIGUNG dessen, dass die vorrangige Rolle des menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten die Bedeutung der Schaffung von Arbeitsplatzkulturen unterstreicht, bei denen der Datenschutz und die Sicherheit organisatorische Prioritäten sind, unter anderem durch die regelmäßige Durchführung von Trainings-, Schulungs- und Sensibilisierungsprogrammen, die Berücksichtigung des Datenschutzes bereits bei der Gestaltung, beim Betrieb und der Verwaltung von Systemen und Praktiken sowie durch die Umsetzung technologischer Lösungen;

Unter HINWEIS DARAUF, dass die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre zuvor festgestellt hat, dass auf globale Strategien, Normen und Modelle hingearbeitet werden muss, und dass für ein höheres Maß an Zusammenarbeit bei der Regulierung gesorgt werden muss, um datenschutzrechtliche Probleme wirksam zu verhüten, zu erkennen, zu bekämpfen und zu beheben, und um die Kohärenz und Vorhersehbarkeit in dem Aufsichtssystem in der Datenwirtschaft zu gewährleisten;

Unter BERÜCKSICHTIGUNG der laufenden Arbeiten der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zur Gewährleistung dessen, dass die digitale Wirtschaft durch die digitale Sicherheit und den Schutz der Privatsphäre gefördert wird, und zur Verbesserung der faktengesicherten Grundlage für die Politikgestaltung in den Bereichen Sicherheit und Schutz der Privatsphäre, einschließlich der Vergleichbarkeit der Berichte über Meldungen von Verletzungen des Schutzes personenbezogener Daten;

In ANBETRACHT der Tatsache, dass die Umfrage der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre aus dem Jahr 2017 gezeigt hat, dass sich die Systeme zur Meldung von Verletzungen des Schutzes personenbezogener Daten in den einzelnen Rechtsordnungen der Mitgliedstaaten unterscheiden, und dass sie über kein System zur Meldung von Verletzungen des Schutzes personenbezogener Daten, über kein freiwilliges Meldesystem zur Meldung von Verletzungen des Schutzes personenbezogener Daten, und über keine verbindlichen Meldepflichten von Verletzungen des Schutzes personenbezogener Daten verfügen, die allgemein

sowie für bestimmte Bereiche gültig sind;[1]

Unter HERVORHEBUNG DER TATSACHE, dass die Erhebung, Klassifizierung, Analyse und Veröffentlichung von Statistiken über Verletzungen des Schutzes personenbezogener Daten, die den Datenschutzbehörden gemeldet wurden, einschließlich ihrer Ursachen, von wesentlicher Bedeutung für die Entwicklung einer globalen Politik und einer Antwort auf die Ursachen von Verletzungen des Schutzes personenbezogener Daten sind;

In ERINNERUNG daran, dass die 31. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre im Jahr 2009 die Internationalen Standards zum Schutz der Privatsphäre (im Folgenden „Entschließung von Madrid“) angenommen hat, die Grundsätze für den Schutz personenbezogener Daten durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen (Grundsatz 20 – Sicherheitsmaßnahmen) und proaktive Maßnahmen einschließlich der regelmäßigen Durchführung von Schulungs- und Sensibilisierungsprogrammen und Prüfungen durch unabhängige Parteien (Grundsatz 22 – proaktive Maßnahmen) umfassen;

Unter HINWEIS DARAUF, dass die 32. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre im Jahr 2010 beschlossen hat, die Annahme von „Privacy by Design“-Grundsätzen als Orientierungshilfe für die Einrichtung des Datenschutz als Standard-Betriebsmodell bei Organisationen zu fördern;

Beschließt die 41. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre folgendes:

1) Die Mitglieder der ICDPPC, die Statistiken über Verletzungen des Schutzes personenbezogener Daten erheben, analysieren und veröffentlichen, die Ihnen im Rahmen eines freiwilligen oder obligatorischen Meldesystems gemeldet wurden, werden zu folgendem aufgerufen:

   (i) Klassifikation der Ursachen von Verletzungen des Schutzes personenbezogener Daten und diesbezügliche Berichterstattung, unter Erwägung der Aufnahme von Klassifikationen derjenigen Verletzungen, die das Ergebnis menschlichen Versagens sind; und

   (ii) Fortsetzung der Prüfung von Empfehlungen von Expertengremien wie der OECD und der ICDPPC-Arbeitsgruppe für Datenschutzindikatoren zur Messung von Verletzungen des Schutzes personenbezogener Daten.

2) Alle Mitglieder der ICDPPC sollen geeignete Sicherheitsvorkehrungen fördern, um menschliches Versagen zu verhindern, das zu Verletzungen des Schutzes personenbezogener Daten führen kann. Diese Aufgabe könnte folgendes umfassen:

   (i) Die Schaffung von Arbeitsplatzkulturen, bei denen der Schutz der Privatsphäre und die Sicherheit der personenbezogenen Daten organisatorische Prioritäten sind, u. a. durch die regelmäßige Durchführung von Trainings-, Schulungs- und

[1] Arbeitsgruppe für Datenschutzindikatoren der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre*: High level results of the ICDPPC Census 2017* (2017) https://icdppc.org/wp- Inhalt/uploads/2017/09/ICDPPC-Census-Report-1.pdf.

Sensibilisierungsprogrammen für Mitarbeiter über ihre Datenschutz- und Sicherheitsverpflichtungen und die Aufdeckung und Meldung von Bedrohungen für die Sicherheit personenbezogener Daten;

(ii) Die Einrichtung solider und wirksamer Verfahren und Systeme für den Datenschutz und den Schutz der Privatsphäre, unter anderem durch:

a. Die Integration des Schutzes der Privatsphäre in die Gestaltung, den Betrieb und in die Verwaltung von Systemen und Praktiken, sowie Investitionen in die Verbesserung der allgemeinen Sicherheitslage im Einklang mit den bekannten Sicherheitsrisiken; und

b. auf der Ebene der Nutzer: Die Umsetzung von Technologien zur Ergänzung der Schulung der Nutzer zwecks Eindämmung des Risikos der unberechtigten Preisgabe von Benutzeranmeldeinformationen und der ungewollten Weitergabe personenbezogener Daten an unberechtigte Empfänger;

(iii) Die Bewertung von Datenschutzpraktiken, Verfahren und Systemen zur Gewährleistung einer dauerhaften Wirksamkeit, unter anderem durch die Umsetzung eines Programms für eine proaktive Überprüfung, einschließlich der Überwachung und Prüfung der Systeme.

3) Alle ICDPPC-Mitglieder sollen sich mit den einschlägigen internationalen und regionalen Netzwerken in Verbindung setzen, um diese Entschließung voranzubringen.

4) Organisationen (einschließlich Regierungen und Unternehmen) sollen begreifen und anerkennen, dass Verletzungen des Schutzes personenbezogener Daten häufig mit menschlichem Irrtum verbunden sind, und sie sollen geeignete Sicherheitsmaßnahmen ergreifen, zu denen auch die in Abschnitt (2) genannten Maßnahmen zählen können.

ERLÄUTERUNG

Diese Resolution ist ein weiterer Schritt in Richtung einer globalen ICDPCC-Strategie zur Verhinderung von Verletzungen des Schutzes personenbezogener Daten, indem der Schwerpunkt auf die Sicherheitsmaßnahmen gelegt wird, die geeignet sind, gegen die Ursache vieler Verletzungen des Schutzes personenbezogener Daten vorzugehen – menschlicher Irrtum.

Der Entwurf einer Entschließung kommt zur rechten Zeit, da aufgrund des deutlichen Anstiegs der Anzahl der Meldungen in den Rechtsprechungen, die Mitgliedsstaaten der ICDPPC sind, und die über ein obligatorisches Systems für die Meldung datenschutzrechtlicher Verletzungen verfügen, bestätigt wird, was seit einiger Zeit bekannt ist, nämlich dass zahlreiche Verletzungen des Schutzes personenbezogener Daten durch menschliches Versagen verursacht oder ausgelöst werden.[2]

[2] Die Ermittlung von menschlichem Versagen als Ursache vieler Verletzungen des Schutzes personenbezogener Daten erfolgte vor dem Zeitpunkt, zu dem die Einführung von Systemen zur Meldung von Verletzungen des

Mit der ersten Aufforderung zur Einreichung von Vorschlägen soll auf der Grundlage der Meldungen der datenschutzrechtlichen Verstöße die Evidenzbasis geschaffen werden. In einer Umfrage aus dem Jahr 2017 über die statistische Praxis bei der Meldung von Verletzungen des Datenschutzes, die in Zusammenarbeit mit der Arbeitsgruppe für Datenschutzindikatoren der ICDPPC durchgeführt wurde, hat sich gezeigt, dass es nur wenige Gemeinsamkeiten bei der Art und Weise gibt, in der die befragten Personen die Ihnen gemeldeten datenschutzrechtlichen Verstöße klassifizierten, und es wurde darauf hingewiesen, dass es gute Arbeitsmöglichkeiten gibt, die Behörden bei der Entwicklung gemeinsamer Verfahren zur Klassifikation von Verstößen zu unterstützen.[3]

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat ähnliche Probleme im Rahmen ihrer laufenden Arbeiten zur Verbesserung der Evidenzbasis für die Politikgestaltung in den Bereichen Sicherheit und Schutz der Privatsphäre festgestellt. Die Arbeit der OECD in diesem Bereich umfasste die Ausarbeitung eines Fragebogens mit Unterstützung der ICDPPC, um eine Machbarkeitsstudie darüber zu erstellen, welche Daten die Datenschutzbehörden erheben und melden sollten, um die Vergleichbarkeit bei der Meldung von Verletzungen des Schutzes personenbezogener Daten zu verbessern. Der Fragebogen enthält auch Überlegungen zu der Klassifizierung von Arten von Datenschutzverletzungen. Es geht insbesondere um die Frage, ob Daten nach obersten Kategorien der Klassifizierungen oder nach spezielleren Unterkategorien nach Art von Vorfällen zu klassifizieren sind.[4]

Die Aufforderung zur Einreichung von Vorschlägen richtet sich nur an diejenigen Mitglieder, die Statistiken über die ihnen gemeldeten Verletzungen von personenbezogenen Daten erheben, analysieren und veröffentlichen, unter Berücksichtigung, dass die Meldesysteme in den einzelnen Rechtsprechungen der einzelnen Mitgliedstaaten unterschiedlich sind, wobei einige Mitgliedstaaten über kein Meldesystem oder über keine Praxis der Berichterstattung zu Statistiken über die ihnen gemeldeten Verletzungen personenbezogener Daten verfügen.

Die zweite Aufforderung zur Einreichung von Vorschlägen richtet sich an alle einzelnen ICDPCC-Mitglieder. Darin wird anerkannt, dass menschliches Versagen überwiegend der Grund ist, und sie fordert die Mitglieder der ICDPPC auf, bei den Organisationen nicht nur die Umsetzung wirksamer IKT-Sicherheitsmaßnahmen zu fördern, sondern auch Maßnahmen zur Bekämpfung des menschlichen Irrtums, um die kontinuierliche Wirksamkeit von IKT-Maßnahmen zu gewährleisten und um sich mit dem Faktor Mensch auseinanderzusetzen.

In der Aufforderung zur Einreichung von Vorschlägen wird eine nicht erschöpfende Liste von

---

Schutzes personenbezogener Daten verpflichtend wurde, und menschliches Versagen wurde als bekannte Ursache von Verletzungen des Schutzes personenbezogener Daten durch die Mitgliedstaaten gemeldet, die freiwillige oder keine Systeme zur Meldung von Verletzungen des Schutzes personenbezogener Daten haben, sowie in Berichten von privaten und Forschungseinrichtungen.

[3] Blair Stewart, *Verbesserung der Messung von Vorfällen im Bereich der digitalen Sicherheit (Perspektiven für die Privatsphäre):Bestandsaufnahme und Handlungsprioritäten* (18. April 2017) https://icdppc.org/wp-content/uploads/2017/04/Breach- Meldestatistik-Erhebungszeitraum 18-April-2017.pdf.

[4] siehe z. B. OECD-Arbeitsgruppe für Sicherheit und Datenschutz in der digitalen Wirtschaft (WPSDE), *Förderung der Vergleichbarkeit von personenbezogenen Daten durch die Meldung:Ergebnisse einer OECD-Erhebung über die Durchsetzung des Schutzes personenbezogener Daten* (13. bis 14. November 2018) DSTI/CDEP/SPDE (2018) 13;OECD WPSPDE, *OECD-Workshop „Improving the Measurement of Digital Security Incidents and Risk Management" (Verbesserung der Messung von Problemen bei der digitalen Sicherheit und Risikomanagement):Entwurf der Zusammenfassung und der wichtigsten* Punkte (30./31. Oktober 2017, Paris) http://www.oecd.org.

Garantien und Konzepten gebilligt, die den Mitgliedern der ICDPPC bekannt sind[5] und die allgemein als angemessene Sicherheitsgarantien unter bestimmten Umständen anerkannt werden, wie Verlust oder unberechtigtem Zugang, Vernichtung, Nutzung, Änderung oder Offenlegung personenbezogener Daten.[6]

Der dritte Aufruf richtet sich an alle ICDPCC-Mitglieder und soll sicherstellen, dass die Entschließung über die einschlägigen internationalen und regionalen Netze vorangebracht wird.

Der vierte Aufruf richtet sich an Organisationen (Regierungen und Unternehmen). Es soll herausgestellt werden, welche Rolle das menschliche Versagen bei Verletzungen des Schutzes personenbezogener Daten spielt, und welche Sicherheitsmaßnahmen angemessen sein können.

Auch wenn keine der in der Entschließung genannten Sicherheitsklauseln für die ICDPCC-Mitglieder neu sein wird, ist ihre Einbeziehung ein weiterer Schritt zu einer globalen Strategie und eine Antwort auf die bekannten Ursachen von Verletzungen des Schutzes personenbezogener Daten.

[5] Siehe beispielsweise die 31. internationale Konferenz der Datenschutzbeauftragten, *Internationale Standards zum Schutz personenbezogener Daten und Privatsphäre* („ Entschließung von Madrid"), Grundsatz 20 – Sicherheitsmaßnahmen und Grundsatz 22 – Vorausschauende Maßnahmen.

[6] Der Grundsatz der Sicherheitsgarantien ist ein zentraler Grundsatz der Privatsphäre, der in den *Leitlinien der OECD für den Schutz des Privatlebens und den grenzüberschreitenden Verkehr personenbezogener Daten* aus dem Jahr 1980 sowie in den 2013 überarbeiteten *Leitlinien der OECD für den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten festgelegt ist.* Der Grundsatz lautet: Personenbezogene Daten sollten durch angemessene Sicherheitsvorkehrungen gegen solche Risiken wie Verlust, unbefugten Zugriff, Vernichtung, Nutzung, Änderung oder Offenlegung von Daten geschützt werden.