JDP
Drapała &
Partners

GLOBAL COMPLIANCE

LOKALE RISIKEN

8 Datenschutz - Hot Spots die in Polen zu beachten sind

Im Folgenden erörtern wir die polnischen Datenschutzbestimmungen und häufige Fehler, die von Unternehmen in Polen begangen werden, wenn ausländische Muttergesellschaften Lösungen einführen. Wir zeigen die möglichen Folgen auf und wie sie durch die Einführung geeigneter Instrumente verhindert werden können.

Inhaltsverzeichnis

1. COOKIES & ANDERE TRACKING-TECHNOLOGIEN

POLNISCHE BESONDERHEITEN

In Polen ist die Verwendung von Cookies und anderen Tracking-Technologien durch das Gesetz über elektronische Kommunikation (Artikel 399-400 GeK) streng geregelt. Gemäß diesen Bestimmungen dürfen Cookies nur mit vorheriger, aktiver und eindeutiger Zustimmung des Nutzers auf dessen Endgerät platziert werden. Der Nutzer muss die Möglichkeit haben, seine Zustimmung zu verschiedenen Kategorien von Dateien (z. B. für den Betrieb des Dienstes, für die Analyse, für das Marketing) getrennt zu erteilen, und er muss in der Lage sein, seine Zustimmung jederzeit problemlos zu widerrufen. Laut Gesetz ist ein Verzeichnis der erteilten Einwilligungen zu erstellen, aus dem hervorgeht wer, wann und in was eingewilligt hat, und es müssen maximale Aufbewahrungsfristen für jede Art von Daten festgelegt werden. Die Aufsichtsbehörde (Amt für elektronische Kommunikation, poln. Urząd Komunikacji Elektronicznej, kurz "UKE" oder die Datenschutzbehörde poln. Urzad Ochrony Danych Osobowych, kurz "UODO") prüft bei einem Audit unter anderem, ob das Einwilligungsbanner die Ablehnung aller Dateien zulässt und ob die Protokolle den Einwilligungsverlauf tatsächlich so archivieren, dass eine vollständige Überprüfbarkeit gewährleistet ist.

TYPISCHER FEHLER

Globales Soft-Opt-In-Banner - eine Schaltfläche „Alle akzeptieren", keine Möglichkeit zum Opt-Out oder zur Deaktivierung von Analysen. Einverständnis wird „durch weitere Überprüfung" anerkannt, kein Einverständnisregister und Tabellen zur Datenaufbewahrung.

MÖGLICHE KONSEQUENZEN

- Strafe des Amtes für Elektronische Kommunikation – bis zu 3 % der in Polen erzielten Einnahmen.
- Strafe Datenschutzamts/DSGVO– bis zu 20 Mio. EUR oder 4% der globalen Umsätze .
- Die sofortige Abschaltung von Skripten kann zu einem Rückgang der Konversionen und zum Verlust von Analysedaten führen.

UNSER VORSCHLAG – VORTEIL FÜR MANDANTEN

Was wir bieten	Konkreter Nutzen
Cookie-Richtlinie EN/EN + Banner für die Zustimmung EN/EN („Ich akzeptiere / Ich lehne ab / Einstellungen")	Konsistentes, annahmefertiges Dokument; einfache Implementierung durch jedes Web-Entwicklungsteam. Beibehaltung einer konsistenten UX der Gruppe bei vollständiger Einhaltung der polnischen Anforderungen.
Checklisten für die vierteljährliche Überprüfung der Einhaltung der Vorschriften	Checklisten für die vierteljährliche Überprüfung der Einhaltung der Vorschriften
Zustimmungsregister + Aufbewahrungsmatrix	Fertiger Nachweis der Verantwortlichkeit zur Vorlage beim Amt für elektronische Kommunikation/Datenschutzamt; Vereinfachung der internen Berichterstattung.
Workshop „Legal Tags in 90 Minuten" für Marketing und IT	Das Team ist in der Lage, die Einhaltung der Vorschriften bei nachfolgenden Kampagnen selbständig aufrechtzuerhalten, was die Zeit bis zur Markteinführung und die Rechtsberatungskosten reduziert.

2. MARKETING-KOMMUNIKATION (E-MAIL, SMS, PUSH, MESSENGER)

POLNISCHE BESONDERHEITEN

Jede Nachricht mit kommerziellem Charakter bedarf - auch wenn sie an eine Geschäftsadresse gesendet wird - der vorherigen ausdrücklichen Zustimmung des Empfängers (Art. 398 GeK).

Erforderliche Zustimmung:

- unabhängig von der Annahme der Nutzungsbedingungen oder der Datenschutzrichtlinie,
- klar dokumentiert (Datum, Uhrzeit, Quelle),
- einfach zu widerrufen und das Unternehmen ist verpflichtet, den Widerruf innerhalb von 48 Stunden zu berücksichtigen,
- getrennt für jeden Kommunikationskanal (z. B. SMS, Push, E-Mail, Telefonanruf).

TYPISCHER FEHLER

Massenhaftes B2B-Cold Calling auf der Grundlage eines „berechtigten Interesses“ oder eines aggregierten Kontrollkästchens, das die Zustimmung zum Marketing kombiniert. Kein zentrales Zustimmungsprotokoll oder Abmeldungshistorie.

POTENZIELLE FOLGEN EINES FEHLERS

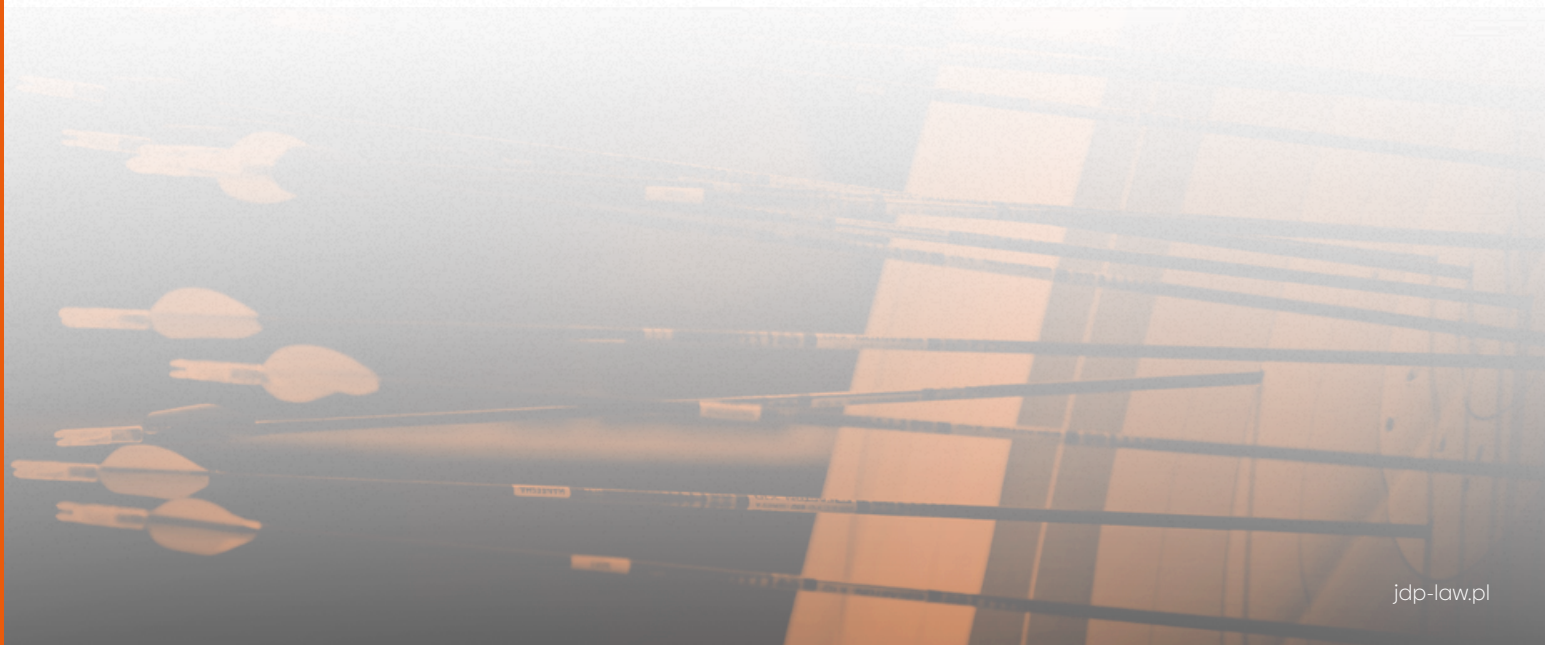
- Strafe des Amtes für elektronische Kommunikation - bis zu 3 % des in Polen erzielten Jahresumsatzes.
- Strafe des Präsidenten des Amts für Wettberwerbs- und Verbraucherschutz für einen Manager wegen vorsätzlichen Verhaltens in Höhe von bis zu 2 Millionen PLN.

Praktische Beispiele:

- Telekommunikationsbetreiber - 9,1 Millionen PLN Strafe für den Versand von mehr als 3,8 Millionen Marketing-SMS ohne die erforderliche Zustimmung der Kunden
- 80.000 PLN Geldstrafe für mehr als 30.000 Werbeanrufe ohne Zustimmung der Empfänger
- Telekommunikationsbetreiber - 2,85 Mio. PLN Strafe (2024) für Telefonanrufe und den Versand von Marketinginhalten per SMS und E-Mail ohne die erforderliche Zustimmung;
- Telekommunikationsbetreiber - 5 Mio. PLN Strafe für Direktmarketing unter Verwendung automatischer Anrufsysteme (SMS-Werbung) ohne Zustimmung der Empfänger, auch wenn die Aktivitäten an ein externes Unternehmen ausgelagert wurden.

UNSER ANGEBOT– MERHWERT FÜR DEN MANDANTEN

Was wir bieten	Konkreter Nutzen
Politik zur Erlangung der Zustimmung + Muster für ein „Präferenzzentrum“ (PL/EN, bereit zur Umsetzung)	Einheitliches, rechtsgültiges Formular mit separaten Kontrollkästchen; der Nutzer sieht klare Wahlmöglichkeiten, was die Konversionsrate erhöht und das Risiko von Verstößen gegen das Gesetz über elektronische Kommunikation minimiert.
Muster eines Zustimmungsregisters mit Anweisungen zur Integration mit einem beliebigen CRM	Jede Zustimmung ist mit Datum, Quelle und Umfang versehen - im Falle einer UKE/UODO-Prüfung exportiert die Rechtsabteilung den Bericht mit einem Klick.
Das Verfahren für den Umgang mit einem Opt-out („Opt-out SLA 48 h“) - Anleitung für Marketing und IT + vorgefertigte E-Mail zur Bestätigung des Opt-out	Die rasche Streichung einer Adresse aus der Liste verringert die Zahl der Beschwerden, schützt den Ruf der Domäne und verringert das Risiko eines hohen Bußgeldes.
Einseitige Checkliste vor der Kampagne (vom Eigentümer der Kampagne zu unterzeichnen)	Die Selbstkontrolle durch das Marketingteam verringert den Bedarf an ständiger rechtlicher Überwachung und beschleunigt den Start neuer Sendungen.
Mini-Schulung online „Opt-in in 30 Minuten” (Aufzeichnung + PDF-Material)	Neue Mitarbeiter verstehen die Regeln schnell und können so die Einhaltung der Vorschriften ohne zusätzliche Einarbeitungskosten sicherstellen.



3. ÜBERWACHUNG VON MITARBEITERN UND BESUCHERN (VIDEOÜBERWACHUNG UND E-MAIL)

POLNISCHE GEGEBENHEITEN

Jede Form der Überwachung am Arbeitsplatz - einschließlich der Bildaufzeichnung mit CCTV-Kameras, der GPS-Standortverfolgung und der Kontrolle von Geschäfts-E-Mails - muss gemäß Artikel 22² des Arbeitsgesetzes förmlich in die Arbeitsordnung aufgenommen werden . Der Arbeitgeber muss die Arbeitnehmer mindestens 14 Tage im Voraus über die geplante Durchführung der Überwachung informieren und entsprechende Schilder in den von der Überwachung betroffenen Bereichen anbringen. Der Zweck der Überwachung muss klar definiert werden (z. B. Gewährleistung der Sicherheit, Schutz des Eigentums, Wahrung der Vertraulichkeit von Informationen), und alle Maßnahmen müssen dem beabsichtigten Zweck angemessen sein und den Datenschutzvorschriften entsprechen.

TYPISCHE FEHLER

Tools zum Scannen von E-Mails, die zentral im Konzern eingesetzt werden, ohne Berücksichtigung des lokalen rechtlichen Umfelds für diese Technologien.
Mitlesen der Post von Mitarbeitern ohne deren Zustimmung durch die IT-Abteilung, ohne dass eine Überwachung eingeführt wird.
CCTV-System ohne klare Beschilderung.
GPS in Fahrzeugen ohne Nutzungsbeschränkung.
Überwachung von Firmentelefonen ohne klare Informationen.

MÖGLICHE KONSEQUENZEN

- Bußgeld der Arbeitsinspektion – bis zu 50 000 PLN
- Sanktionen durch Datenschutzbehörde (z.B. 160.000 EUR für die verdeckte Überwachung einer medizinischen Einrichtung);
- Entschädigungsansprüche von Arbeitnehmern wegen Verletzung der Persönlichkeitsrechte oder Privatsphäre
- Folgen der Verwendung von illegalem Überwachungsmaterial in Rechtsstreitigkeiten mit Arbeitnehmern prüfen
- Mögliche strafrechtliche Sanktionen: Geldstrafe, Freiheitsbeschränkung Freiheitsstrafe von bis zu 2 Jahren (Artikel 267 § 3 des Strafgesetzbuchs).

UNSER ANGEBOT – MEHRWERT FÜR DEN MANDANTEN

Was wir bieten	Konkreter Nutzen
DPIA-Bewertung und Aktualisierung der Arbeitsvorschriften (CCTV + E-Mail)	Die Überwachung wird nach polnischem Recht geregelt - die Beweise sind im Streitfall ohne das Risiko von Regressansprüchen gültig.
Musterzeichen, Klauseln und Zeitplan für die Löschung der Aufzeichnungen	Der Arbeitnehmer wird ordnungsgemäß informiert, wodurch sich das Risiko von Beschwerden an die Arbeitsinspektion und UODO verringert.
Zugangsprotokoll für E-Mail-Postfächer	Die Personalabteilung/Rechtsabteilung verfügt über ein klares, genehmigtes Verfahren - Vorwürfe der „unbefugten Überwachung“ werden vermieden.

4. PRIVATE GERÄTE UND MESSENGER (BYOD)

POLNISCHE GEGEBENHEITEN

In der polnischen Rechtsordnung darf ein Arbeitgeber die Verarbeitung von Geschäftsdaten auf den privaten Geräten der Mitarbeiter nur zulassen, nachdem er die schriftliche Zustimmung der Mitarbeiter eingeholt und eine angemessene Risikobewertung durchgeführt hat, wobei die Anforderungen der DSGVO und Artikel 22[1] des Arbeitsgesetzes zu berücksichtigen sind. Außerdem müssen MDM-Lösungen (Mobile Device Management) oder andere Sicherheitsmechanismen für private Geräte implementiert werden, und das Kündigungsverfahren muss die Wiederherstellung oder Löschung von Unternehmensdaten auf diesen Geräten regeln.

TYPISCHER FEHLER

Die Mitarbeiter nutzen ihre privaten Telefone und Computer für geschäftliche Zwecke (BYOD), das Unternehmen hat jedoch keine festgelegte Richtlinie oder schriftliche Genehmigung für diese Regelung (kein MDM). Diese Geräte sind nicht angemessen gesichert und es gibt kein Verfahren zur Wiederherstellung der darauf gespeicherten Unternehmensdaten, wenn ein Mitarbeiter das Unternehmen verlässt.

MÖGLICHE KONSEQUENZEN

- DSGVO Geldbuße i.H.v. 4% des globalen Umsatzes
- Mögliche strafrechtliche Haftung der Verantwortlichen (Artikel 107 des Datenschutzgesetzes) für die Bereitstellung von Daten an Unbefugte.
- Verlust der Kontrolle über Betriebsgeheimnisse (z. B. Kunden-datenbank auf privatem Laufwerk).

UNSER ANGEBOT – MEHRWERT FÜR DEN MANDANTEN

Was wir bieten	Konkreter Nutzen
BYOD-Richtlinie und Messenger + Muster für Einverständnis-erklärungen	Mitarbeiter und Führungskräfte verfügen über klare Richtlinien, die das Risiko von Datenverlusten minimieren.
Liste der MDM-/ Verschlüsselungs-anforderungen + Playbook „Verlorenes Telefon“	Der mobile Vorfall wird schnell eingedämmt, was Sie davor bewahren kann, der Datenschutzbehörde gemeldet und mit einer Geldstrafe belegt zu werden.
Workshop „Secure Messaging”	Das Vertriebs- und Kundendienstteam setzt Kommunikatoren in einer Weise ein, die mit dem Gesetz und den Anforderungen der Branche übereinstimmt.

5. HINWEISGEBER (WHISTLEBLOWING)

POLNISCHE GEGEBENHEITEN

Das polnische Whistleblowing-Gesetz aus dem Jahr 2024 schreibt vor, dass alle Meldungen von Hinweisgebern von einer speziellen, in Polen tätigen Stelle entgegengenommen und bearbeitet werden. Die Organisation muss sicherstellen, dass angemessene organisatorische und technische Sicherheitsvorkehrungen getroffen werden, und wenn eine externe SaaS-Plattform verwendet wird, sollte sie zusätzliche Vereinbarungen treffen, um sicherzustellen, dass Whistleblowing in Übereinstimmung mit polnischem Recht bearbeitet wird und dass der Hinweisgeber rechtzeitig eine Rückmeldung erhält.

TYPISCHER FEHLER

Ein Meldekanal, der ausschließlich in der Zentrale (z. B. in Deutschland) funktioniert, ohne lokale Verfahren, ohne polnisches Entscheidungsteam und ohne rechtzeitige Rückmeldung.

MÖGLICHE KONSEQUENZEN

- Ordnungsgeld von bis zu 50.000 PLN für Verfahrensmängel oder Fehlfunktionen.
- Strafrechtliche Verantwortung (Geldstrafe, Freiheitsbeschränkung, bis zu 3 Jahren Haft) für Vergeltungsmaßnahmen.
- Imagekrise nach der Bekanntgabe an die Medien oder externe Stellen.

UNSER ANGEBOT – MEHRWERT FÜR DEN MANDANTEN

Was wir bieten	
Globale Kanalortung (DPIA, PL-Verfahren, Register der Anmeldungen)	Das Unternehmen erfüllt die Anforderungen des Gesetzes, ohne seine gesamte IT-Plattform ersetzen zu müssen.
Schulung des Meldeaus-schusses	Entscheidungen werden schnell und rechtmäßig getroffen, wodurch kriminelle und Reputationsrisiken minimiert werden.
„Dry-run" – Test des Vorfalls	Das Team kennt das Verfahren in der Praxis und Lücken werden vor dem realen Einsatz behoben.

6. DATENSCHUTZRICHTLINIEN UND NAMENTLICHE BERECHTIGUNGEN

POLNISCHE GEGEBENHEITEN

Die Aufsichtsbehörde (UODO) betont in ihren Entscheidungen immer wieder, dass jeder Mitarbeiter über eine Genehmigung zur Verarbeitung personenbezogener Daten verfügen muss, die den Umfang der Tätigkeiten und die Systeme enthält, die er bearbeiten darf. Die Datenschutzichtlinie sollte die Organisationsstruktur des Unternehmens widerspiegeln, die für die Bearbeitung von Anfragen betroffener Personen zuständigen Rollen (Reaktionszeit - 30 Tage) und das Verfahren für das Management von Zwischenfällen (Reaktion bis zu 72 Stunden) festlegen und in jedem Unternehmen gesondert umgesetzt werden. Diese Dokumentation ist ein wichtiger Nachweis der Verantwortlichkeit im Falle eines Audits.

TYPISCHER FEHLER

Globale Politik, die „per E-Mail" umgesetzt wird, ohne Beschluss des Vorstands eines polnischen Unternehmens und ohne Einzelgenehmigungen; kein Vorfallregister.

MÖGLICHE KONSEQUENZEN

- UODO-Entscheidung über 40 000 PLN wegen fehlender Unterlagen und Anordnung, die Datenverarbeitung bis zur Vervollständigung einzustellen.
- Operationelles Chaos bei einem Vorfall - das Fehlen klarer Rollen verlangsamt die Reaktion und erhöht das Risiko finanzieller Sanktionen.
- In der Praxis des Datenschutzamtes werden die meisten Strafen für das Versäumnis verhängt, Verstöße zu dokumentieren und die Betroffenen zu benachrichtigen. Beispiel: Geldstrafe von über 363.000 PLN für eine Bank, weil sie es versäumt hatte, ihre Kunden über ein Datenschutzleck zu informieren.

UNSER ANGEBOT – MEHRWERT FÜR DEN MANDANTEN

Was wir bieten	Konkreter Nutzen
Editierbares, skalierbares Vollmachtsformular (Word/Excel)	Das Unternehmen erfüllt die Anforderungen des Gesetzes, ohne seine gesamte IT-Plattform ersetzen zu müssen.
Vorstandsbeschluss + aktualisierte Datenschutz-Politik	Entscheidungen werden schnell und rechtskonform getroffen, wodurch strafrechtliche und rufschädigende Risiken minimiert werden.
Überprüfung der Gruppenverfahren und „local overlay" - Tabelle der Diskrepanzen PL vs. Globalstandard	Das Team kennt das Verfahren in der Praxis, und Lücken werden vor der eigentlichen Anwendung geschlossen.
Verfahren zur Ausübung der Rechte von Personen und Ereignisregister (Workflow + Registerblatt)	Ein klarer, genehmigter Ablauf von Anfragen und Ereignissen verkürzt die Reaktionszeiten, verringert das Risiko von Strafen bei Verzögerungen und ermöglicht eine Berichterstattung an den Vorstand in einem klaren Format.

7. DATENSCHUTZBEAUTRAGTER(DSB)

POLNISCHE GEGEBENHEITEN

In Polen muss der DSB eine natürliche Person sein, die der gegenüber der Datenschutzbehörde von einem polnischen Unternehmen ernannt wird. Wird eine externe Organisation mit dieser Aufgabe betraut, muss ein bestimmter Mitarbeiter dieser Organisation als verantwortlicher DSB benannt werden. Seine oder ihre Kontaktdaten - einschließlich Vor- und Nachname - müssen in polnischer Sprache auf der Website und in den Informationsklauseln angegeben werden. Der DSB sollte direkt dem Vorstand unterstellt sein und über die notwendigen Ressourcen verfügen, um seine Aufgaben zu erfüllen; er sollte Polnisch sprechen oder von einem polnischsprachigen Team unterstützt werden.

TYPISCHER FEHLER

Eine Person, die als globaler DSB fungiert, wurde in Polen nicht förmlich gemeldet; keine Kontaktdaten auf Polnisch auf der Website; der DSB nimmt auch andere Aufgaben wahr - Interessenkonflikt.

MÖGLICHE KONSEQUENZEN

- DPA-Geldbuße i.h.v. 25.000 PLN (Beispiel 2024) wegen Nichtanmeldung des DSB
- Mögliche Strafen von bis zu 2 % des weltweiten Umsatzes (DSGVO) bei schwereren Verstößen.
- Anordnung zur Bestellung eines neuen DSB und erneute Unterrichtung aller betroffenen Personen.

UNSER ANGEBOT – MEHRWERT FÜR DEN MANDANTEN

Was wir bieten	Konkreter Nutzen
DSB Anmeldung on-line in 24 h	Das Risiko einer Strafe wegen Nichtregistrierung wird sofort beseitigt.
Outsourcing-Vertrag oder „Shadow-DSB-Support“	Der globale DSB erhält sprachliche und operative Unterstützung von uns, ohne dass er eine neue Person einstellen muss.
Jahresplan für die Arbeit des DSB + KPI-Dashboard	Das Management erhält messbare Berichte über die Einhaltung der Vorschriften, was die Aufsicht und Haushaltsentscheidungen erleichtert.

8. JÄHRLICHE DATENSCHUTZPRÜFUNG

POLNISCHE GEGEBENHEITEN

Gemäß dem Grundsatz der Rechenschaftspflicht in Artikel 24 der DSGVO ist jedes Unternehmen verpflichtet, jährlich oder nach jeder wesentlichen Änderung in der IT-Gegebenheiten (z. B. neues System, Unternehmensübernahme) eine dokumentierte Bewertung der Wirksamkeit der getroffenen Datenschutzmaßnahmen durchzuführen. Das Datenschutzamt verlangt in seinen Entscheidungen einen vom Vorstand genehmigten Auditbericht mit Empfehlungen für Abhilfemaßnahmen als Grundlage für den Nachweis der vollständigen Einhaltung der Vorschriften bei einer möglichen Kontrolle.

TYPISCHER FEHLER

Die im Jahr 2023 eingeführten Maßnahmen wurden nicht aktualisiert, und neue Anträge
und Lieferanten wurden überhaupt nicht bewertet; das interne Audit beschränkt sich auf eine „copy-paste“-Checkliste.

MÖGLICHE KONSEQUENZEN

- Veraltete Verfahren führen dazu, dass Vorfälle nicht entdeckt oder zu spät gemeldet werden.
- Die maximale DSGVO-Strafe beträgt je nach Verstoß entweder 2 % oder 4 % des Gesamtumsatzes.

UNSER ANGEBOT – MEHRWERT FÜR DEN MANDANTEN

Was wir bieten	Konkreter Nutzen
Risikobasierte Prüfungsmethodik und 12-Monats-Zeitplan	Eine Überprüfung, die auf die tatsächlichen Risiken des Unternehmens zugeschnitten ist, und nicht nur eine „Papierformalität“.
Arbeitsblatt "Audit in 60 Minuten - Selbsteinschätzung der Abteilungen”	Die einzelnen Abteilungsleiter können die Einhaltung der Vorschriften schnell intern bewerten; das zentrale Datenteam erhält standardisierte Ergebnisse, ohne dass langwierige Besprechungen erforderlich sind.
Table-Top-Workshop mit dem Vorstand	Das Management probt das Kontroll- oder Störfallszenario, was die Reaktionszeit in einer kritischen Situation verkürzt.

KONTAKT

Anna Matusiak-Wekiera

Radczyni prawna (Rechtsanwältin PL)
Counsel
Head of Data Protection & Compliance

anna.matusiak-wekiera@jdp-law.pl

Krzysztof Brant

Radca prawny (Rechtsanwalt PL)
Senior Associate
Data Protection & Compliance

krzysztof.brant@jdp-law.pl

JDP Drapała & Partners

JDP DRAPAŁA & PARTNERS Sp. k. / KRS: 0001145849/ Registergericht: Amtsgericht für die Hauptstadt Warschau, XII. Wirtschaftsabteilung des Landesgerichtsregisters / NIP: 7010056483 / REGON: 140887753