Uriach

Globale Datenschutzrichtlinie

Dokument	**Globale Datenschutzrichtlinie**
Zweck	Festlegung von Zielen und Kriterien für die Verarbeitung personenbezogener Daten.
Genehmigender	Risiko- und Compliance-Ausschuss ("**CRC**")

Vertraulichkeit - Die Verteilung dieses Dokuments ist auf alle Unternehmen der Uriach-Gruppe und ihre Geschäftspartner beschränkt. Es darf nicht ohne die Zustimmung des Verwaltungsrats weitergegeben werden.

00 DEFINITION

Die in dieser Globalen Datenschutzrichtlinie (die "**Richtlinie**") verwendeten Begriffe haben die in der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG ("**DSGVO**") festgelegte Bedeutung, es sei denn, in dieser Richtlinie wird ausdrücklich eine andere Bedeutung angegeben.

01 ZWECK

Mit dieser Richtlinie soll sichergestellt werden, dass jedes Unternehmen von Uriach die anwendbaren Datenschutzbestimmungen einhält, d. h. die DSGVO und die lokalen Bestimmungen in jedem Gebiet, in dem Uriach tätig ist (die "**anwendbaren Datenschutzbestimmungen**").

Diese Richtlinie wird an Gesetzesänderungen in den Ländern, in denen Uriach tätig ist, sowie an die von der örtlich zuständigen Aufsichtsbehörde, dem Europäischen Datenschutzausschuss ("**ECDC**") und den Urteilen der zuständigen Gerichte festgelegten Kriterien angepasst.

02 BEREICH

Der Anwendungsbereich dieser Richtlinie umfasst folgendes:

a) **Unternehmensbereich** - Diese Richtlinie gilt für alle Unternehmen, die zu Uriach gehören, sowie für Tochter- und Beteiligungsgesellschaften, über die Uriach die tatsächliche Kontrolle ausübt oder Positionen in den Leitungsorganen innehat.
b) **Personal** - Diese Richtlinie gilt für alle Ebenen der Organisation, einschließlich der Geschäftsleitung, des oberen Managements, der Aufsichtsorgane und aller Mitarbeiter.
c) **Geschäftsbeziehungen** - Der Geltungsbereich dieser Richtlinie erstreckt sich, soweit möglich, auf Lieferanten, Kunden, Unterauftragnehmer und Mitarbeiter.
d) **Geografischer Geltungsbereich** - Diese Richtlinie gilt für alle geografischen Gebiete, in denen Uriach Niederlassungen unterhält, unabhängig davon, ob es sich um lokale oder internationale Niederlassungen handelt.

Ausnahmen von den in dieser Richtlinie dargelegten Regeln bedürfen der ausdrücklichen Genehmigung des Risiko- und Compliance-Ausschusses ("**CRC**"). Bei Unstimmigkeiten oder Fragen im Zusammenhang mit dieser Richtlinie werden von der Rechtsabteilung einschlägige Hinweise und Unterstützung angeboten.

03 GESCHÄFTLICHE VERARBEITUNGSTÄTIGKEITEN UND RISIKEN

Die Haupttätigkeit von Uriach liegt im Bereich des Gesundheitswesens. Die häufigsten Verarbeitungen personenbezogener Daten in diesem Sektor sind die folgenden:

1. Personalrekrutierung
2. Mitarbeiterverwaltung
3. Beziehungen zu B2C-Kunden
4. Beziehungen zu B2B-Kunden
5. Beziehungen zu den Lieferanten
6. Marketing
7. Kundenbetreuung
8. Pharmakovigilanz, Kosmetovigilanz
9. Klinische Versuche, Beobachtungsstudien
10. e-Commerce

11. Finanzen
12. Rechtliches

Die Hauptrisiken, die sich aus der Nichteinhaltung der in den geltenden Datenschutzbestimmungen festgelegten rechtlichen Verpflichtungen ergeben, sind die folgenden:

13. Verwaltungsrechtliche Sanktionen
14. Regulatorische Intervention
15. Fragen der Qualität
16. Schadenersatz
17. Reputationsschaden
18. Verstöße gegen die Privatsphäre

Der Schutz personenbezogener Daten ist für Uriach ein vorrangiges Ziel und erfordert eine Reihe rechtlicher, technischer und organisatorischer Maßnahmen, die in dieser Richtlinie zusammengefasst sind und in den einschlägigen Unternehmensvorschriften, Protokollen und/oder Verfahren festgelegt werden.

04 GRUNDSÄTZE DES DATENSCHUTZES

a) **Rechtmäßigkeit**: Es werden nur personenbezogene Daten verarbeitet, für die Uriach eine gesetzlich festgelegte legitime Grundlage hat.

b) **Transparenz**: Uriach informiert die betroffenen Personen in klarer und einfacher Weise über alle Umstände der Verarbeitung.

c) **Fairness**: Uriach darf personenbezogene Daten nicht unter anderen als den angegebenen Umständen verarbeiten.

d) **Zweckbindung**: Uriach sammelt personenbezogene Daten für festgelegte, eindeutige und rechtmäßige Zwecke und verarbeitet sie nicht in einer Weise weiter, die mit diesen Zwecken unvereinbar ist.

e) **Datensparsamkeit**: Personenbezogene Daten müssen dem Zweck entsprechen, für den sie verarbeitet werden, dafür erheblich sein und sich auf das beschränken, was für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

f) **Korrektheit**: Personenbezogene Daten müssen sachlich richtig sein und erforderlichenfalls auf dem neuesten Stand gehalten werden, und Uriach ergreift alle angemessenen Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die in Bezug auf die Zwecke, für die sie verarbeitet werden, unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

g) **Begrenzung der Speicherung**: Uriach speichert personenbezogene Daten in einer Form, die die Identifizierung der betroffenen Personen ermöglicht, nicht länger, als es für die Zwecke, für die sie erhoben wurden, erforderlich ist.

h) **Integrität und Vertraulichkeit**: Uriach verarbeitet personenbezogene Daten in einer Weise, die eine angemessene Sicherheit durch die Anwendung geeigneter technischer und organisatorischer Maßnahmen gewährleistet. Personenbezogene Daten sind nur Personen zugänglich, die zum Zugriff auf sie berechtigt sind, und dürfen

nicht ohne entsprechende Genehmigung und Rechtsgrundlage an Dritte weitergegeben werden.

i) **Rechenschaftspflicht**: Jedes Unternehmen von Uriach ist für die Einhaltung der Bestimmungen der jeweils anwendbaren DV-Vorschriften verantwortlich und muss in der Lage sein, diese Einhaltung nachzuweisen.

j) **Datenschutz bei der Planung und bei der Voreinstellung**: In der Planungsphase neuer Verarbeitungen, Projekte, Dienstleistungen und Produkte, bei denen personenbezogene Daten verarbeitet werden, führt Uriach eine vorherige Bewertung der Auswirkungen auf den Datenschutz durch.

05 KONTROLLORGANE, AUFGABEN UND ZUSTÄNDIGKEITEN

Alle Mitarbeiter von Uriach, unabhängig von ihrer Position, sind verpflichtet, die Regeln, Verfahren und Kontrollen einzuhalten, die zur Einhaltung der geltenden Datenschutzbestimmungen festgelegt wurden.

Das Governance-Modell, das die gute Leistung von Uriach im Bereich des Datenschutzes sicherstellen soll, ist folgendes:

a) **Globaler Datenschutzausschuss**: Der Globale Datenschutzausschuss ist dafür verantwortlich, dass die vorliegende Richtlinie durch die Umsetzung der verschiedenen vorgesehenen Maßnahmen wirksam wird.

Dem globalen Datenschutzausschuss gehören als ständige Mitglieder die Personen aus Uriach an, die zu einem bestimmten Zeitpunkt das Amt des Datenschutzbeauftragten innehaben:

- Chief Legal & Sustainability Officer - Vorsitzender
- Legal & Compliance Manager und ernannter DSB in den zentralen Dienststellen - Sekretär
- Global Data &Technology Director - Mitglied
- Cybersecurity Spezialist - Mitglied
- Global Digital & Data Director - Mitglied

Von den Mitgliedern des Globalen Datenschutzausschusses wird erwartet, dass sie ihre Kenntnisse über die einschlägigen rechtlichen und regulatorischen Anforderungen auf dem neuesten Stand halten, zusätzliche Vorschriften zur Umsetzung dieser Richtlinie fördern und Schulungen für alle Mitarbeiter anbieten.

b) **Lokale Datenschutzbeauftragte:** Je nach den lokalen Erfordernissen und der geltenden Gesetzgebung können lokale Datenschutzbeauftragte (DSB) ernannt und den zuständigen Aufsichtsbehörden offiziell benannt werden. Diese lokalen Datenschutzbeauftragten müssen dem Globalen Datenschutzausschuss Bericht erstatten und sind für die Einhaltung der Datenschutzbestimmungen in ihrem jeweiligen Hoheitsgebiet verantwortlich.

c) **Mitglieder der Organisation:** Alle Mitglieder der Organisation sind für die Einhaltung der geltenden Datenschutzbestimmungen und für die korrekte Entwicklung der Richtlinie verantwortlich.

Alle Mitglieder der Organisation, unabhängig von ihrer Position, können:

- die Einhaltung der Bestimmungen dieser Richtlinie zu gewährleisten,
- unverzüglich auf Hinweise zu reagieren, die sie vom Globalen Datenschutzausschuss erhalten, und
- wenden Sie sich an den Globalen Datenschutzausschuss, wenn Sie Fragen zur Auslegung dieser Richtlinie oder zur Anwendung der geltenden Datenschutzbestimmungen haben.

Ebenso müssen alle Mitglieder der Organisation den Globalen Datenschutzausschuss unverzüglich über jede Maßnahme zur Verhinderung oder Behebung eines möglichen Verstoßes gegen die vorliegende Richtlinie informieren.

06 REGISTER DER VERARBEITUNGSTÄTIGKEITEN

Jedes Unternehmen von Uriach führt ein Verzeichnis der Verarbeitungstätigkeiten ("**RAT**"). Die in diesem RAT enthaltenen Verarbeitungen sind das Ergebnis einer Analyse, die durch Befragung aller Abteilungen, die in Ausübung ihrer Tätigkeit personenbezogene Daten verarbeiten können, durchgeführt wird.

Der RAT wird regelmäßig aktualisiert, um ein aktuelles Bild der von den einzelnen Unternehmen von Uriach durchgeführten Verarbeitungen zu vermitteln.

07 RECHTE DER BETROFFENEN PERSONEN

Jedes Unternehmen von Uriach erleichtert die Ausübung der Rechte der betroffenen Personen, wenn es entweder als für die Verarbeitung Verantwortlicher oder als Auftragsverarbeiter handelt. Außerdem müssen sie geeignete Regeln, Verfahren oder Protokolle in Bezug auf die oben genannten Punkte einführen.

08 KONTROLLE DER LIEFERANTEN

Das Genehmigungsverfahren für Uriach-Lieferanten umfasst eine Vorabprüfung, um unter anderem zu bestätigen, ob der betreffende Lieferant die Verarbeitung personenbezogener Daten benötigt, um seine Dienstleistungen oder Waren bereitzustellen.

Zu diesem Zweck hilft die Vorabprüfung bei der Auswahl der Lieferanten und der Durchführung eines Vorabbewertungs- und Genehmigungsverfahrens.

Jedes Unternehmen von Uriach kann Regeln und Verfahren zur Entwicklung, Spezifizierung und Detaillierung des Inhalts dieses Abschnitts aufstellen. Insbesondere, aber nicht ausschließlich, setzt jedes Unternehmen von Uriach nur Auftragsverarbeiter ein, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so umgesetzt werden, dass die Verarbeitung den Anforderungen der anwendbaren Datenschutzvorschriften entspricht und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

09 INTERNATIONALE TRANSFERS

Uriach übermittelt personenbezogene Daten an ein Drittland oder eine internationale Organisation außerhalb des Europäischen Wirtschaftsraums ("**EWR**") nur auf der Grundlage von:

1. eine Entscheidung über die Angemessenheit;
2. geeignete Schutzmaßnahmen wie Standardvertragsklauseln ("**SCC**");
3. verbindliche Unternehmensregeln

4. eine Genehmigung der zuständigen Aufsichtsbehörde; oder
5. Ausnahmeregelungen für besondere Situationen.

10 DATENSPEICHERFRISTEN

Die Uriach-Unternehmen speichern personenbezogene Daten so, dass die betroffenen Personen nur so lange identifiziert werden können, wie es für die Zwecke, für die die Daten verarbeitet werden, erforderlich ist.

Die Unternehmen erstellen und aktualisieren ein Schema, in dem die Aufbewahrungsfrist für die Daten festgelegt ist, die sie gemäß den jeweiligen geltenden Datenschutzbestimmungen aufbewahren müssen oder für angemessen halten. In diesem Schema sind die Verjährungsfristen für Verstöße und die in den anwendbaren Datenschutzbestimmungen festgelegten Beschränkungen zu berücksichtigen, ebenso wie gesetzliche, sektorale und vertragliche Verpflichtungen, die längere Aufbewahrungsfristen erfordern können.

Die Unternehmen von Uriach informieren die betroffenen Personen über die Aufbewahrungsfristen, wenn ihre Daten erhoben werden.

11 DATENSCHUTZ-FOLGENABSCHÄTZUNG ("DPIA")

Die Uriach-Gesellschaften beurteilen die Notwendigkeit einer Datenschutzfolgenabschätzung gemäß den jeweils geltenden Datenschutzbestimmungen und führen sie gegebenenfalls vor Beginn der jeweiligen Datenverarbeitungstätigkeit durch.

12 DATENSCHUTZBEAUFTRAGTER ("DPO")

Jedes Unternehmen von Uriach nimmt eine Bewertung der Notwendigkeit der Bestellung eines DSB gemäß den jeweils geltenden Datenschutzbestimmungen vor.

Die Notwendigkeit, einen DSB zu bestellen, ist dem Globalen Datenschutzausschuss (dpo@uriach.com) unverzüglich mitzuteilen

13 SICHERHEITSMASSNAHMEN

Jedes Unternehmen von Uriach hat geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein den Risiken angemessenes Sicherheitsniveau zu gewährleisten. Zu diesen Zwecken muss jede Organisation den Stand der Technik, die Kosten der Umsetzung und die Art, den Umfang, den Kontext und die Zwecke der Verarbeitung sowie das Risiko mit unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen berücksichtigen.

14 DATENVERLETZUNGEN UND RISIKOKOMMUNIKATION

Uriach wird Protokolle für den Umgang mit Datenschutzverletzungen einführen und sicherstellen, dass geeignete Maßnahmen sowohl präventiv als auch reaktiv ergriffen werden, und erforderlichenfalls die zuständigen Aufsichtsbehörden innerhalb von 72 Stunden benachrichtigen und/oder die Verletzung den betroffenen Personen mitteilen.

Jede Verletzung des Datenschutzes ist dem Globalen Datenschutzausschuss unverzüglich mitzuteilen.

15 DATENSCHUTZ-AUDIT

Uriach führt in regelmäßigen Abständen Audits durch, um die in dieser Richtlinie genannten Risiken zu bewerten und die Einhaltung der jeweils geltenden DV-Vorschriften sicherzustellen.

Bei dieser Prüfung kann es sich um eine interne, externe oder gemischte Prüfung handeln, bei der das Vorhandensein, die Angemessenheit und die Wirksamkeit der Maßnahmen und Kontrollen zur Verhinderung von Verstößen gegen die Vorschriften über den Schutz personenbezogener Daten überprüft wird.

Der Umfang dieses Audits unterscheidet sich von dem der Folgenabschätzung insofern, als sich die Folgenabschätzung auf einen bestimmten Verarbeitungsvorgang bezieht, während sich das Datenschutzaudit auf die Einhaltung der geltenden Datenschutzvorschriften in der gesamten Organisation bezieht.

16 AUSBILDUNG UND SENSIBILISIERUNG

Uriach fördert die ständige Schulung und Sensibilisierung für den Datenschutz auf allen Ebenen der Organisation, um das Bewusstsein der Organisation für den Schutz personenbezogener Daten zu verbessern.

Die vorgenannten Maßnahmen werden entweder im Rahmen von Präsenzveranstaltungen oder von E-Learning-Kursen oder anderen Arten von Kommunikations- und Schulungsmaterialien und -instrumenten durchgeführt, um das Bewusstsein für die Risiken von Verstößen auf allen Ebenen der Organisation zu schärfen.

17 DIE AKTUALISIERUNG UND UMSETZUNG DIESER RICHTLINIE

Diese Richtlinie und ihre Umsetzung werden regelmäßig überprüft. Jede Änderung muss vom CRC genehmigt werden

* * *