Datenschutzerklärung für die Personalmanagement Plattform „X.on“

1. Verantwortlicher und Geltungsbereich

Diese Erklärung gilt für innerhalb der Plattform genutzten Fachanwendungen und Funktionen (bAV, Personalakte, PayReader, App my xon) sowohl in der Web-Applikation als auch über die iOS- und Android Apps.

Für die Verarbeitung von Personaldaten im Rahmen der Personalverwaltung ist grundsätzlich der Arbeitgeber (nachfolgend **X.on Company**), also das jeweilige Unternehmen, das X.on einsetzt, Verantwortlicher im Sinne der DSGVO. Die X.on GmbH handelt hierfür als Auftragsverarbeiter gemäß Art. 28 DSGVO auf Grundlage eines Auftragsverarbeitungsvertrags (AVV). Beschäftigte wenden sich für Betroffenenrechte (Art. 15–22 DSGVO) primär an ihren Arbeitgeber bzw. dessen Datenschutzbeauftragten.

Versicherungsvermittler wie bspw. Versicherungsmakler nutzen X.on als zertifizierte X.on partner zur Unterstützung bei bAV-Prozessen. Je nach Ausgestaltung können X.on partner eigenständige Verantwortliche sein oder als Auftragsverarbeiter des Arbeitgebers agieren. Soweit X.on partner eigenständig über Zwecke und Mittel entscheiden, veröffentlichen sie eigene Datenschutzhinweise. Bei einer Auftragsverarbeitung erfolgt die Verarbeitung auf Grundlage eines AVV zwischen Arbeitgeber und X.on partner.

Daneben wird die X.on GmbH im Rahmen der Bereitstellung des Dienstes als eigenständig Verantwortlicher tätig. Sie erreichen uns unter:

X.on GmbH (nachfolgend X.on)
Angermunder Straße 126
40489 Düsseldorf-Angermund

E-Mail: backoffice@xon.online
Telefon: +49 (0) 174 333 555 1

Unseren Datenschutzbeauftragten erreichen Sie:

postalisch unter:
dhpg IT-Services GmbH, z. Hd. Herrn Dr. Christian Lenz
Bunsenstr. 10a
51647 Gummersbach

per E-Mail unter:
datenschutz@dhpg.de

telefonisch unter:
+49 2261 8195 0

2. Kategorien personenbezogener Daten

- Nutzungs- und Protokolldaten (Log-Ins, Rollen / Rechte, Zeitstempel, IP-Adresse, Geräte- / App-Informationen, Fehlerberichte),
- Support-/Kommunikationsdaten (Supporttickets, E-Mails/Telefonnotizen, Inhalte aus Rückmeldungen),
- App-spezifische Daten: gerätespezifische Kennungen (z.B. für Push-Benachrichtigungen), Berechtigungen (Dateizugriff, Kamera / Foto für Uploads; nur nach Einwilligung des Nutzers / Berechtigungsfreigabe).

---

3. Zwecke und Rechtsgrundlagen

Wir verarbeiten diese Daten zu den folgenden Zwecken:

3.1 Web-Anwendung

- Betrieb, Sicherheit, Missbrauchsprävention, Logging, Skalierung, Backups: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an sicherem Betrieb).
- Fehleranalyse/Produktverbesserung (aggregiert/anonymisiert): Art. 6 Abs. 1 lit. f DSGVO; wo nötig Art. 6 Abs. 1 lit. a DSGVO (Einwilligung, z. B. optionale Nutzungsanalyse).
- Lizenz-/Nutzungsabrechnung & Vertragserfüllung ggü. Kunden: Art. 6 Abs. 1 lit. b DSGVO und lit. f (Missbrauchsprävention).
- Erfüllung rechtlicher Pflichten (z. B. steuerliche Aufbewahrung, Compliance-Meldungen): Art. 6 Abs. 1 lit. c DSGVO.
- Kommunikation/Support gegenüber Kunden und autorisierten Nutzer:innen: Art. 6 Abs. 1 lit. b bzw. lit. f (Kundenbetreuung).

3.2 Mobile App, Berechtigungen & Push

- Geräteberechtigungen (Kamera/Dateien) nur für Uploads/Downloads, sofern vom Nutzer aktiviert; Rechtsgrundlage: Art. 6 Abs. 1 lit. b (funktional erforderlich) bzw. lit. a (sofern optional).
- Push-Benachrichtigungen: Art. 6 Abs. 1 lit. a DSGVO (Einwilligung, jederzeit in den App-Einstellungen widerrufbar).

3.3 Cookies (Web)

Auf der Plattform X.on kommen ausschließlich technisch erforderliche Cookies und vergleichbare Speicherungstechniken zum Einsatz, um den Betrieb der Plattform sicherzustellen. Konkret nutzt X.on drei temporäre Cookies (Session-Cookies) namens „XSRF-TOKEN“, „laravel_session“ und „JSESSIONID“. Diese Cookies sind notwendig, um Ihre Benutzersitzung aufrechtzuerhalten und die Sicherheit der Anwendung zu gewährleisten. Insbesondere dienen sie dem Sitzungs-Management (d.

h. dem Erkennen Ihres Logins innerhalb der Web-App) und dem Schutz vor sogenannten Cross-Site-Request-Forgery-Angriffen (CSRF; einem Angriff auf Web-Sessions, vor dem das XSRF-TOKEN-Cookie schützt). Die Verarbeitung dieser technisch notwendigen Cookies erfolgt auf Grundlage unseres berechtigten Interesses an einem sicheren, funktionsfähigen Dienst (Art. 6 Abs. 1 lit. f DSGVO sowie § 25 Abs. 2 Nr. 2 TDDDG).

Zusätzlich verwendet X.on den lokalen Speicher (Local Storage) Ihres Browsers für bestimmte technische Funktionen. Hierbei handelt es sich nicht um Cookies im engeren Sinne, sondern um eine lokale Speicherfunktion Ihres Webbrowsers. Darin werden z. B. Interface-Daten temporär vorgehalten, um die Bedienung der Anwendung zu erleichtern. Die im Local Storage abgelegten Informationen verbleiben ausschließlich auf Ihrem Endgerät und werden nicht an unseren Server übertragen. Sie sind technisch notwendig für die Funktionsfähigkeit der Web-App (§ 25 Abs. 2 Nr. 2 TDDDG) und werden automatisiert nach ca. 4 Stunden gelöscht.

Drittanbieter-Cookies oder sonstige nicht erforderliche Cookies, für die wir Ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO, § 25 Abs. 1 TDDDG benötigen würden, werden nicht eingesetzt. Wir binden keine externen Analyse- oder Marketingdienste ein und verwenden ausschließlich lokale Ressourcen. Das bedeutet, dass alle für X.on benötigten Inhalte wie Skripte, Bilder oder Schriftarten von unseren eigenen Servern geladen werden. Es werden keine Cookies durch externe Anbieter (z. B. Google, Social-Media-Plug-ins oder Werbenetzwerke) über unsere Anwendung gesetzt. Ebenso verzichten wir vollständig auf Tracking- oder Profiling-Cookies.

---

4. Empfänger und Kategorien von Auftragsverarbeitern

Die Empfänger der Daten sind

Hosting/Cloud & Rechenzentrumsbetrieb
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur

Mail/Kommunikationsdienste
unternehmen online GmbH & Co. KG, Freie-Vogel-Straße 371, 44269 Dortmund

Backup/Logging
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur

Monitoring
unternehmen online GmbH & Co. KG, Freie-Vogel-Straße 371, 44269 Dortmund

Plattformwartung und -entwicklung
unternehmen online GmbH & Co. KG, Freie-Vogel-Straße 371, 44269 Dortmund

KI-gestützte Dokumentenverarbeitung und Analyse
Microsoft Ireland Operations Limited, One Microsoft Place, South County, Business Park, Carmanhall And Leopardstown, Dublin, D18 P521, Irland

Elektronische Signaturen
signotect GmbH, Am Gierath 20 b, 40885 Lintorf

Alle Auftragsverarbeiter werden nach **Art. 28 DSGVO** vertraglich gebunden. **Empfänger** im

Rahmen gesetzlicher Pflichten können Behörden, Gerichte oder Steuer-/Sozialversicherungsträger sein.

---

5. Drittlandübermittlungen

Eine Übermittlung in Drittländer (außerhalb EU/EWR) findet nur statt, wenn dies zur Leistungserbringung erforderlich ist oder Sie eingewilligt haben und angemessene Garantien nach Art. 44 ff. DSGVO bestehen (z. B. EU-Standardvertragsklauseln, ergänzende Transfer Impact Assessments, Zusatzmaßnahmen).

---

6. Speicherdauer

Wir verarbeiten personenbezogene Daten **nur so lange**, wie es für die Zwecke erforderlich ist oder gesetzliche Aufbewahrungspflichten bestehen. Die für uns relevanten Fristen lauten:

- Protokolle/Logs/Sicherheitsdaten: 12 Monate (bedarfsgerecht, IT-Sicherheit/Missbrauchsprävention)
- Support-/Kommunikationsdaten: 3 Jahre

---

7. Betroffenenrechte

Sie haben das Recht:

- gemäß Art. 15 DSGVO Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten zu verlangen. Sofern wir Ihre Daten verarbeiten, können Sie insbesondere Auskunft über die Verarbeitungszwecke, die Kategorie der personenbezogenen Daten, die Kategorien von Empfängern, gegenüber denen Ihre Daten offengelegt wurden oder werden, insbesondere bei Empfängern in Drittländern, die geplante Speicherdauer oder die Kriterien für deren Festlegung, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde, die Herkunft ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten verlangen;
- gemäß Art. 16 DSGVO unverzüglich die Berichtigung unrichtiger oder Vervollständigung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen;
- gemäß Art. 17 DSGVO die Löschung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen, soweit nicht die Verarbeitung insbesondere zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist;

- gemäß Art. 18 DSGVO die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, soweit die Richtigkeit der Daten von Ihnen bestritten wird, die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen und wir die Daten nicht mehr benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen oder Sie gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung eingelegt haben und noch nicht feststeht, ob unsere berechtigten Gründe gegenüber Ihren Interessen überwiegen;
- gemäß Art. 20 DSGVO Ihre personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen, sofern die Verarbeitung auf Ihrer Einwilligung oder einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt;
- gemäß Art. 7 Abs. 3 DSGVO Ihre einmal erteilte Einwilligung jederzeit gegenüber uns zu widerrufen. Dies hat zur Folge, dass wir die Datenverarbeitung, die auf dieser Einwilligung beruhte, für die Zukunft nicht mehr fortführen dürfen und

Die zuständige Aufsichtsbehörde im Land Nordrhein-Westfalen ist:

Landesbeauftragte für Datenschutz und Informationsfreiheit
Kavalleriestraße 2–4
40213 Düsseldorf
Deutschland
Telefon: +49 211 38424-0
Fax: +49 211 38424-10
E-Mail: poststelle@ldi.nrw.de

---

8. Änderungen dieser Datenschutzerklärung

Wir können diese Erklärung anpassen, wenn dies aufgrund rechtlicher, technischer oder betrieblicher Änderungen erforderlich ist. Es gilt die jeweils aktuelle Fassung in der Anwendung. Wesentliche Änderungen werden wir in geeigneter Weise mitteilen.