Datenschutz-Richtlinie

Wir, die ***InnoFly Unternehmensfamilie***, sind uns der Bedeutung des Schutzes persönlicher Daten bewusst und verpflichten uns, die Privatsphäre unserer Mitarbeiter, Kunden und Geschäftspartner zu respektieren und zu schützen. In dieser Richtlinie erläutern wir die wesentlichen Inhalte der Datenschutz-Grundverordnung (DSGVO), wie wir mit den Vorgaben dieser Richtlinie umgehen und wie wir den Datenschutz innerhalb der Unternehmensfamilie pflegen.

1 Warum ist die Datenschutz-Richtlinie wichtig?

Als Teil unseres Unternehmens trägt jeder von uns ***Verantwortung*** dafür, dass wir die Privatsphäre unserer Kunden, Partner und Mitarbeiter respektieren und schützen. Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) ist nicht nur eine gesetzliche Verpflichtung, sondern auch ein zentrales Element unseres ethischen Engagements und unseres professionellen Verhaltens.

Die DSGVO gibt klare Richtlinien vor, wie personenbezogene Daten zu behandeln sind, und bietet gleichzeitig den betroffenen Personen umfassende Rechte. Ein Verstoß gegen diese Vorschriften kann zu erheblichen Bußgeldern führen und das Vertrauen in unser Unternehmen nachhaltig schädigen. Darüber hinaus könnten rechtliche Schritte folgen, die unser Unternehmensimage und unsere Marktstellung beeinträchtigen würden.

Es wird daher an alle Mitarbeiter appelliert, den Datenschutz ernst zu nehmen und aktiv an der Umsetzung der Datenschutzmaßnahmen mitzuwirken. Zu den entsprechenden Maßnahmen gehört:

- Das regelmäßige ***Lesen und Verstehen unserer Datenschutzrichtlinie.***
- Die ***sofortige Meldung*** jeglicher verdächtiger Aktivitäten oder Sicherheitslücken, die personenbezogene Daten gefährden könnten.
- Die ***kontinuierliche Schulung und Sensibilisierung*** bezüglich der neuesten Datenschutzbestimmungen und Praktiken.
- Die ***strikte Einhaltung des Umgangs mit Daten und Anfragen***, um sicherzustellen, dass diese vertraulich und sicher bleiben.

2 Allgemeines zur DSGVO

Die ***Datenschutz-Grundverordnung*** (DSGVO) ist ein Regelwerk, das darauf abzielt, die Daten der Bürger in der Europäischen Union zu schützen. Diese Verordnung ist immer dann anwendbar, wenn personenbezogene Daten einer Person, die sich in der EU befindet, verarbeitet werden. Es spielt keine Rolle, ob das Unternehmen, das die Daten verarbeitet, seinen Sitz in der EU oder außerhalb hat. Sobald es um Daten von Personen geht, die sich in der EU aufhalten, kommt die DSGVO ins Spiel. Auch Amazon (amerikanisches Unternehmen), das Waren in Europa anbietet, unterliegt somit der DSGVO.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das können Daten wie Name, Adresse, Telefonnummer, E-Mail-Adresse, Geburtsdatum, IP-Adresse oder biometrische Merkmale sein. Gemäß der Datenschutz-Grundverordnung (DSGVO) müssen diese Daten besonders geschützt werden, da sie Rückschlüsse auf eine konkrete Person zulassen.

Datenverarbeitung im Sinne der DSGVO umfasst jede Art von Vorgang, der mit persönlichen Daten einer Person durchgeführt wird. Dies schließt Aktionen wie das Sammeln, Speichern, Organisieren, Verwenden, Übermitteln oder Löschen dieser Daten ein.

Stellen wir uns vor, du klickst eine Box an, dass du die Zusendung des Newsletters eines Unternehmens akzeptierst. Du stimmst also zu, dass deine E-Mail-Adresse dafür verwendet

und gespeichert werden darf. Dieses Unternehmen führt verschiedene Tätigkeiten mit deiner E-Mail-Adresse durch:

- ***Sammeln***: Sie erfassen deine E-Mail-Adresse.
- ***Speichern***: Sie speichern sie in ihrer Datenbank.
- ***Verwenden***: Sie verwenden die Adresse, um dir die Newsletter zu senden.
- ***Löschen***: Wenn du entscheidest, dass du keine Newsletter mehr möchtest und dies dem Unternehmen mitteilst, löschen sie deine E-Mail-Adresse aus ihrer Datenbank.

All diese Tätigkeiten fallen unter den Begriff "Datenverarbeitung". Die DSGVO stellt sicher, dass bei all diesen Schritten deine Daten sicher gehandhabt werden und du Kontrolle darüber hast, was mit ihnen geschieht.

Aktuelles Beispiel aus der Praxis	
Vorfall	Werbung ohne wirksame Einwilligung
Strafe	1,2 Millionen €

3 Warum ist die Einhaltung der DSGVO so wichtig?

Der Schutz personenbezogener Daten ist nicht nur eine ***rechtliche Verpflichtung***, sondern auch ein ***Zeichen des Respekts*** gegenüber der Privatsphäre von Einzelpersonen. Die Einhaltung der DSGVO zeigt, dass ein Unternehmen verantwortungsbewusst mit den Daten umgeht, was das Vertrauen von Kunden, Mitarbeitern und Partnern stärkt. Bei Nichteinhaltung können jedoch erhebliche Konsequenzen drohen, darunter:

- ***Bußgelder***: Unternehmen können mit Geldstrafen von bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes belegt werden, je nachdem, welcher Betrag höher ist.
- ***Reputationsverlust***: Datenschutzverletzungen können das Image eines Unternehmens stark schädigen, was zu Kundenverlust und negativer Presse führen kann.
- ***Rechtliche Konsequenzen***: Betroffene Personen können rechtliche Schritte einleiten, wenn sie glauben, dass ihre Daten unrechtmäßig behandelt wurden.

Grundsätzlich haftet der Arbeitgeber für Fehler seiner Mitarbeiter gegenüber Dritten. Innerhalb eines Arbeitsverhältnisses gibt es jedoch gesetzlich spezielle Haftungsregeln. Durch den sogenannten innerbetrieblichen Schadensausgleich wird bei einem Fehlverhalten des Mitarbeiters die ***Verantwortung zwischen Arbeitnehmer und Arbeitgeber aufgeteilt*** und das bezahlte Bußgeld durch den Arbeitgeber vom Mitarbeiter rückgefordert.

Verstöße gegen Datenschutzregeln können ernsthafte ***arbeitsrechtliche Folgen*** haben, wie Abmahnungen oder sogar Kündigungen. Beispielsweise hat das Landesarbeitsgericht Köln entschieden, dass das Lesen und Ausdrucken einer offensichtlich an einen Kollegen gerichteten E-Mail, sowie das Kopieren und Weitergeben privater Chatverläufe eines Kollegen an Dritte, eine sofortige fristlose Kündigung rechtfertigen kann.

Ein weiteres Urteil des Landesarbeitsgerichts Berlin-Brandenburg aus dem Jahr 2016 bestätigte, dass auch das massenhafte Abrufen von Meldedaten durch eine Mitarbeiterin aus Neugier eine fristlose Kündigung rechtfertigen kann, selbst wenn nur wenige Personen davon betroffen sind.

Aktuelles Beispiel aus der Praxis	
Vorfall	Verhängte Sanktion bei intransparenter Datenschutzbestimmung
Strafe	bis zu 7 Millionen €

4 Welche Rechte haben Betroffene, deren Daten bei uns gespeichert sind?

Die DSGVO räumt Einzelpersonen in der EU verschiedene Rechte ein, um ihnen die Kontrolle über ihre persönlichen Daten zu geben. Hier sind diese Rechte einfach erklärt:

- ***Recht auf Auskunft***: Betroffene können eine Bestätigung verlangen, ob persönliche Daten, die sie betreffen, verarbeitet werden. Wenn dies der Fall ist, können sie eine Kopie dieser Daten anfordern und Informationen darüber erhalten, wie und zu welchen Zwecken die Daten verarbeitet werden.
- ***Recht auf Berichtigung***: Sind die gespeicherten Daten unvollständig oder fehlerhaft, haben Betroffene das Recht, deren Berichtigung oder Vervollständigung zu verlangen.
- ***Recht auf Löschung*** (Recht auf Vergessenwerden): Unter bestimmten Bedingungen können Betroffene die Löschung ihrer Daten fordern. Dies gilt vor allem dann, wenn die Daten für die ursprünglichen Verarbeitungszwecke nicht mehr notwendig sind oder wenn die Einwilligung zur Verarbeitung zurückgezogen wurde.
- ***Recht auf Einschränkung der Verarbeitung***: Betroffene können unter bestimmten Umständen verlangen, dass die Verarbeitung ihrer Daten eingeschränkt wird. Dies bedeutet, dass die Daten zwar gespeichert bleiben, aber nicht weiterverarbeitet werden dürfen.
- ***Recht auf Datenübertragbarkeit***: Betroffene haben das Recht, ihre Daten in einem strukturierten, weit verbreiteten und maschinenlesbaren Format zu erhalten. Sie haben auch das Recht, diese Daten an einen anderen Verantwortlichen übertragen zu lassen, ohne von der Organisation, die die Daten bereitstellt, daran gehindert zu werden.
- ***Widerspruchsrecht***: Betroffene können der Verarbeitung ihrer Daten widersprechen, insbesondere wenn diese zu Marketingzwecken oder aufgrund einer spezifischen Situation erfolgt.
- ***Beschwerderecht*****:** Betroffenen Personen wird das Recht zuerkannt, sich bei der Aufsichtsbehörde (in Österreich: Datenschutzbehörde, Barichgasse 40-42 1030 Wien, E-Mail: dsb@dsb.gv.at) zu beschweren, wenn sie der Ansicht sind, dass eine Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt.

Aktuelles Beispiel aus der Praxis	
Vorfall	inkorrekter Negativauskunft und Nicht-Einhaltung der Antwortfrist
Strafe	46.500 €

5 Technische & organisatorische Sicherheitsmaßnahmen

Aufgrund der DSGVO sind Unternehmen verpflichtet, technische und organisatorische Sicherheitsmaßnahmen zu ergreifen, um die personenbezogenen Daten ihrer Kunden, Mitarbeiter und Geschäftspartner zu schützen. Diese Maßnahmen dienen dazu, Daten vor unbefugtem Zugriff, Verlust oder Missbrauch zu bewahren.

Hier sind die wichtigsten Verpflichtungen, die sich daraus ergeben:

- ***Zugangskontrolle***: Es muss sichergestellt sein, dass nur autorisierte Personen Zugang zu den Daten haben. Dies kann durch Passwortschutz, biometrische Erkennung oder Sicherheitskarten erfolgen.
- ***Datensicherung***: Regelmäßige Backups der Daten sind unerlässlich. Diese Backups sollten an sicheren Orten aufbewahrt und verschlüsselt werden, um im Falle eines Datenverlusts eine Wiederherstellung zu ermöglichen.
- ***Verschlüsselung***: Sensible Daten sollten sowohl bei der Übertragung als auch bei der Speicherung verschlüsselt werden, um sie vor unbefugtem Zugriff zu schützen.
- ***Überwachung und Protokollierung***: Unternehmen müssen die Zugriffe auf personenbezogene Daten überwachen und protokollieren, um mögliche Sicherheitsvorfälle nachvollziehen zu können.

- ***Schulung und Sensibilisierung***: Mitarbeiter müssen regelmäßig über Datenschutzrichtlinien und den sicheren Umgang mit personenbezogenen Daten informiert und geschult werden.
- ***Datenschutz-Folgenabschätzung***: Für bestimmte Datenverarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellen, müssen Unternehmen eine DSFA durchführen und dokumentieren.
- ***Notfallmanagement***: Es sollte ein Plan vorhanden sein, der Maßnahmen bei Datenpannen und Sicherheitsvorfällen definiert. Dies umfasst die Benachrichtigung der betroffenen Personen und der zuständigen Datenschutzbehörde innerhalb von 72 Stunden.

Jeder Mitarbeiter trägt ***Verantwortung für den Schutz der Daten***. Ein einziger Fehler oder eine Unachtsamkeit kann schwerwiegende Konsequenzen haben. Indem alle Mitarbeiter sensibilisiert und geschult sind, wird das Risiko solcher Fehler minimiert. Bei einem Sicherheitsvorfall ist es wichtig, dass alle Mitarbeiter wissen, wie sie reagieren müssen und welche Schritte zu unternehmen sind. Ein gut informiertes und koordiniertes Team kann schnell und effizient handeln, um Schäden zu begrenzen und die Einhaltung der gesetzlichen Meldepflichten sicherzustellen.

Die erfolgreiche Umsetzung dieser Maßnahmen hängt entscheidend von der Zusammenarbeit aller Mitarbeiter ab. ***Datenschutz*** ist nicht nur die Verantwortung der IT-Abteilung oder des Datenschutzkoordinators, sondern ***betrifft jeden einzelnen Mitarbeiter*** im Unternehmen.

Aktuelles Beispiel aus der Praxis	
Vorfall	Verhängte Sanktion bei unzureichenden technischen und organisatorischen Sicherheitsmaßnahmen
Strafe	bis zu 5 Millionen €

6 Data-Breach-Notification Duty

Wenn bekannt wird, dass personenbezogene Daten durch ein Sicherheitsdefizit der getroffenen technischen und organisatorischen Maßnahmen hervorgerufen werden (=***Datenpanne***), müssen diese Betroffenen unverzüglich informiert werden.

Der Datenmissbrauch kann aufgrund der folgenden Ereignisse eintreten:

- Unbefugter Zugriff auf Daten, z.B. durch Außentäter (Hacking-Angriff) oder nicht berechtigte Mitarbeiter
- Diebstahl von IT-Komponenten und Datenträgern (PCs, Notebooks, USB-Sticks, Papierdokumente, Ausdrucke,...)
- Verlust von IT-Komponenten und Datenträgern (Notebooks, USB-Sticks, Smartphones,...)
- Fehlerhafte Adressierung, Versendung von Mails an einen großen Verteiler mit „cc“ statt „bcc“

Weiters ist für das Vorliegen einer meldepflichtigen Datenpanne erforderlich, dass objektiv eine Verletzung des Schutzes personenbezogener Daten eingetreten ist. Der Verdacht allein reicht nicht. Nicht entscheidend ist, ob tatsächlich von den Daten Kenntnis von einem Dritten genommen wurde.

Zu beachten ist, dass der Schaden nicht bereits eingetreten sein muss. Es genügt die Möglichkeit, dass zukünftig daraus ein Schaden (in finanzieller Hinsicht, in Bezug auf das Ansehen oder hinsichtlich einer körperlichen Gefährdung der Betroffenen) entstehen könnte. Dieser muss allerdings auch schwerwiegend sein, ein voraussichtlich geringfügiger Schaden führt nicht zum Entstehen einer Informationspflicht.

Wenn eine Datenpanne vorliegt, so muss dies der Datenschutzbehörde, als auch den Betroffenen ***binnen 72 Stunden*** mitgeteilt werden. Die Meldefrist beginnt ***ab*** dem Zeitpunkt zu laufen, ab dem irgendjemand in dem Unternehmen ***Kenntnis*** von den erheblichen Tatsachen der Datenpanne erhalten hat. Diese Frist gilt auch am Wochenende und selbst bei Feiertagen, wie Ostern und Weihnachten. Daher ist bei Kenntnis derartiger Tatsachen ***unverzüglich der Datenschutzkoordinator zu informieren***.

Die Information der Betroffenen kann grundsätzlich in jeder möglichen Form erfolgen. Abgesehen von direkten Kommunikationsformen, z.B. durch Brief- oder E-Mail-Versand, ist auch die Veröffentlichung in Tageszeitungen denkbar.

Aktuelles Beispiel aus der Praxis	
Vorfall	Verhängte Sanktion bei Verspätung der 72 Stunden Meldepflicht
Strafe	bis zu 500 000 €

7 Umgang mit Anfragen zum Datenschutz

Die Beantwortung von Anfragen bzw. Beschwerden hinsichtlich des Datenschutzes obliegt dem Datenschutzkoordinator. Eingehende Anfragen sind umgehend an datenschutz@innofly.at weiterzuleiten.

Im Falle von an euch gerichtete Auskunftsersuchen beachtet bitte unbedingt nachfolgende Richtlinien:

- ***Grundsatz der Datengeheimhaltung***: Die Erteilung von Auskünften ist grundsätzlich verboten, außer es gibt eine rechtliche Grundlage für die Zulässigkeit der Datenweitergabe.
- ***Keine Auskunft ohne rechtliche Grundlage***: Seid ihr euch hinsichtlich der Zulässigkeit der Auskunftserteilung unsicher, verlangt bitte von der anfragenden Stelle die Bekanntgabe der rechtlichen Grundlage für die Auskunftserteilung (z.B. eine passende Gesetzesstelle oder einen Gerichtsbeschluss). Wenn euch keine eindeutig nachvollziehbare Rechtsgrundlage genannt wird, verweigert die Auskunft unter Hinweis auf das Datengeheimnis. Dies gilt auch dann, wenn die anfragende Stelle z.B. eine Behörde ist, da auch öffentliche Ämter und Behörden an das Datenschutzgesetz gebunden sind.
- ***Keine telefonische Auskunft***: Auskünfte per Telefon sind – wenn euch der Gesprächspartner nicht persönlich bekannt ist – jedenfalls unzulässig, da nicht mit Sicherheit verifizierbar ist, wer sich am anderen Ende der Leitung befindet (Missbrauchsgefahr).
- ***Umgang mit besonders drängenden Anfragen***: Lasst euch auch im Falle von unangenehm drängenden Anfragern nicht zu einer sofortigen Auskunft hinreißen, sondern verweist den Anfrager höflich darauf, dass die Auskunft ohne nachweisliche Legitimation nicht möglich ist (besonderes Drängen könnte eine bewusste Taktik des Anfragers sein).
- ***Grundsatz der Verhältnismäßigkeit***: Die Auskunft hat sich auf die unbedingt notwendigen Punkte zu beschränken. Informationen, die für die angefragte Auskunft nicht erforderlich sind, dürfen nicht mitgeteilt werden.

Für weiterführende Fragen sowie zur Abklärung bei Unklarheiten oder Zweifelsfragen steht euch gerne unser ***Datenschutzkoordinator Alexander Gisy*** zur Verfügung:

E-Mail: datenschutz@innofly.at
Telefon: 0660 6233407

Fahrplan für Datenpannen gem. Art 33 DSGVO

Was ist meldepflichtig?	Liegt vor?	
1. Datenpanne ist **durch ein Sicherheitsdefizit der getroffenen technischen und organisatorischen Maßnahmen** hervorgerufen worden. Beispiele: rechtswidrige Datenübermittlung an Dritte, versehentliche fehlerhafte Adressierung, Versendung von Mails an einen großen Verteiler mit „cc“ und ohne „bcc“ **Achtung!** Basiert die Verletzung des Schutzes personenbezogener Daten nicht auf einem Defizit der technischen/organisatorischen Maßnahmen, dann liegt **keine meldepflichtige Datenpanne** vor.	**Ja** ☐	**Nein** ☐
2. Die Datenpanne hat zu einer a. **Vernichtung**, b. einem **Verlust**, c. einer **Veränderung**, d. zur **unbefugten Offenlegung** oder e. zum **unbefugten Zugang personenbezogener Daten** geführt. Es handelt sich also um eine Vertraulichkeits-, Integritäts- oder Verfügbarkeitsverletzung.	**Ja** ☐	**Nein** ☐
3. **Verletzungserfolg ist objektiv eingetreten**. Der Verdacht allein reicht nicht. Die Meldepflicht besteht dann, wenn ein Zugriff auf die Daten erfolgt ist, unabhängig davon, ob dieser unbeabsichtigt oder beabsichtigt erfolgt. Nicht entscheidend ist, ob tatsächlich von den Daten Kenntnis genommen wurde. **Achtung!** Wollen wir einer Meldepflicht trotz vorliegendem Sicherheitsdefizit entgehen, müssen wir belegen, dass kein Zugriff auf die Daten erfolgte.	**Ja** ☐	**Nein** ☐
4. **Entfall der Meldepflicht an Betroffene?** Eine Benachrichtigung des Betroffenen ist nicht erforderlich, wenn durch nach der Datenpanne ergriffene Maßnahmen das „**hohe Risiko** für die Rechte und Freiheiten der betroffenen Personen“ **nicht mehr besteht** (vgl. Art. 34 Abs. 3 Buchst. b DSGVO). Zu beachten ist allerdings, dass, auch wenn der Betroffene aus o.g. Gründen nicht zu benachrichtigen ist, eine **Meldepflicht gegenüber der Datenschutzaufsichtsbehörde** nach Art. 33 DSGVO nach wie vor besteht! Das Risiko bemisst sich aus der Relation zwischen Schwere des möglichen Schadens und seiner Eintrittswahrscheinlichkeit. Je höher der anzunehmende Schaden ist, desto geringer sind die Anforderungen an die Wahrscheinlichkeit. **Keine Meldepflicht besteht, wenn:** - die Daten ohnehin öffentlich verfügbar sind, - die Daten wirksam verschlüsselt sind (außer es ist ein dauerhafter Datenverlust eingetreten, weil z.B. der einzige Datenträger verloren wurde und es keine Backups gibt) - beim versehentlichen Versand von Daten an eine vertrauenswürdige Drittpartei ist eine Verletzung, jedoch manifestiert sich darin kein Risiko für die Rechte und Freiheiten natürlicher Personen, wenn eine Drittpartei als Berufsgeheimnisträger zur Vertraulichkeit verpflichtet ist **und** die Daten löscht bzw. zurücksendet		

Beurteilung der Kriterien **Wie hoch ist das Risiko, dass durch die Datenpanne entstanden ist?**	**Hohes Risiko**	**Mittleres Risiko**	**Kleines Risiko**
Art des Data Breach (Unautorisierter Zugriff ist oft gravierender als Datenverlust)	☐	☐	☐
Identifizierbarkeit (Wie einfach und wahrscheinlich ist es, dass ein Dritter, der unautorisierten Zugriff nimmt, den Personenbezug herstellen kann?)	☐	☐	☐
Art und Umfang der Daten	☐	☐	☐
Anzahl der Betroffenen	☐	☐	☐
Spezielle Umstände hinsichtlich der Betroffenen (z.B. Kinder, Behinderungen)	☐	☐	☐
Spezielle Umstände hinsichtlich des Verantwortlichen (z.B. Medizinische Einrichtung)	☐	☐	☐
Anzahl der Betroffenen	☐	☐	☐
Zu erwartende Konsequenzen: Zu den Konsequenzen nennt Erwägungsgrund 85 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 - Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile	**Einschätzung:**		

Dokumentation der Datenpanne (egal ob meldepflichtig oder nicht)	**Erledigt?**
1. Zeitlicher Ablauf der Datenpanne	☐
2. Beschreibung der Datenpanne	☐
3. Ausmaß der Datenpanne	☐
4. Folgen für betroffene Personen	☐
5. Maßnahmen zur Minimierung des Schadens	☐
6. Risikoanalyse	☐

Wurde die Datenpanne gemeldet?	**Erledigt?**
Die Meldefrist beginnt ab dem Zeitpunkt zu laufen, ab dem irgendjemand in dem Unternehmen des Verantwortlichen Kenntnis von den erheblichen Tatsachen der Datenpanne erhalten hat. Diese Frist gilt auch am Wochenende und selbst bei hohen Feiertagen, wie Ostern und Weihnachten. Unberücksichtigt bleibt bei der Fristberechnung auch Urlaub und Krankheit.	☐ Datum: Von: An: