RISIKOFOLGENABSCHÄTZUNG DER BAUID

DEIN
DIGITALER
SERVICE
AM BAU

Inhalt

RISIKOFOLGENABSCHÄTZUNG DER BAUID – ZUSAMMENFASSENDE VERSION ZUR VERÖFFENTLICHUNG AUF DER WEBSITE.

Soweit personenbezogene Bezeichnungen nur in männlicher oder weiblicher Form angeführt sind, beziehen sie sich auf alle Geschlechter in gleicher Weise.

1. VORBEMERKUNG

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, **so hat der Verantwortliche** vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten nach Art 35 DSGVO durchzuführen.

Zu prüfen ist vorab, ob die BauID-Software unter einen Ausnahmetatbestand der Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV) fällt, oder ob eine Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V) besteht.

Die BauID-Software unterliegt keinem Ausnahmetatbestand gemäß Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV).

Gemäß § 2 Abs 3 der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), ist eine Datenschutz-Folgenabschätzung verpflichtend durchzuführen, wenn ein Verarbeitungsvorgang zwei oder mehr der nachstehenden Kriterien erfüllt:

- Umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO
- umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO,
- Erfassung von Standortdaten im Sinne des § 92 Abs. 3 Z 6 Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I. Nr. 70/2003, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben,
- Verarbeitung von Daten schutzbedürftiger betroffener Personen, wie unmündige Minderjährige, **Arbeitnehmer**, Patienten, psychisch Kranker und Asylwerber, wobei Abs. 2 letzter Satz sinngemäß anzuwenden ist, oder
- Zusammenführung und/oder Abgleich von Datensätzen aus zwei oder mehreren Verarbeitungen, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt wurden, im Rahmen einer Datenverarbeitung, die über die von einer betroffenen Person üblicherweise zu erwartenden Verarbeitungen hinausgeht, sofern

diese für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei der betroffenen Person erhoben wurden.

Im vorliegenden Fall ist eine Datenschutz-Folgenabschätzung zu erstellen, da eine Verarbeitung von Daten schutzbedürftiger betroffener Personen (Arbeitnehmer) vorgenommen wird, sowie eine Zusammenführung und/oder Abgleich von Datensätzen aus zwei oder mehreren Verarbeitungen, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt werden.

Festgehalten wird, dass keine Pflicht zur Veröffentlichung der Risikofolgenabschätzung besteht. Vielmehr würde die Veröffentlichung der implementierten Maßnahmen zur Datensicherheit selbst ein Sicherheitsrisiko darstellen. Bei dem vorliegenden Dokument handelt sich daher um eine zusammenfassende Version, welche auf der Website der BauID veröffentlicht wird.

2. KONTEXT

2.1 Überblick

2.1.1. Software-Anforderungen

Die Software hat insbesondere folgende Anforderungen zu erfüllen:

- Bereitstellung einer modernen Softwarelösung mit größtmöglicher modularer Softwarearchitektur unter Gewährleistung einer hohen Flexibilität und Erweiterbarkeit, leichter Wartbarkeit und Portabilität, ausgerichtet auf einen mehrjährigen Software-Lifecycle,
- Ablage von Dokumenten,
- automatische Datenlöschung (zur Einhaltung datenschutzrechtlicher Vorschriften),
- Preisstruktur für BUAG-pflichtige Nutzer und nicht- BUAG-pflichtige Nutzer
- Einsicht Finanzpolizei (Schnittstelle)
- Einsicht OEGK (Schnittstelle)
- Einsicht BUAK (Schnittstelle)
- Einsicht Arbeitnehmer in die Abfrageprotokolle
- NFC-Card und Barcode
- Arbeitnehmer deaktivieren
- Arbeitnehmer von einem Bauvorhaben vorübergehend bis zur Herstellung des gesetzlichen Zustands ausschließen (Blacklist)
- Arbeitnehmer in ein Bauvorhaben bis zur nächsten Überprüfung integrieren (Whitelist),
- Protokollführung über Wechsel des Sozialversicherungsträgers
- elektronische Schnittstelle zu Sozialversicherungsträgern
- elektronische Schnittstelle zum BMI
- elektronische Schnittstelle zur BUAK
- elektronische Schnittstelle zum AMS
- modulare Sicherheitsunterweisung
- Verwaltung von Bauvorhaben
- Verwaltung von Arbeitnehmer
- Inventarverwaltung (Schlüsselausgabe)
- zentrale Identitätsprüfung
- Ausstellung einer BauID Karte für Arbeitnehmer

- Zuordnung der Arbeitnehmer zu den einzelnen Bauvorhaben
- App für IOS und Android

2.1.4. Nutzung der Software

Der Hauptzweck der Einführung des Systems liegt in der **Bekämpfung von Sozialbetrug auf Baustellen.** Die Nutzung der Software bzw die Verwendung der BauID-Karte auf den Bauvorhaben soll die Durchführung der notwendigen (**tägliche) Kontrollen auf Baustellen zeitsparend und effizient** ermöglichen.

Die Nutzung des Systems ist freiwillig. Um das System nutzen zu können ist sowohl für Arbeitgeber als auch für Arbeitnehmer der Abschluss einer Nutzungsvereinbarung (Registrierung im System) erforderlich. Arbeitgeber und Arbeitnehmer, die dem Anwendungsbereich des BUAG unterliegen, schließen die Nutzungsvereinbarung mit der BUAK, Arbeitgeber und Arbeitnehmer, die dem System nicht unterliegen schließen die Nutzungsvereinbarung mit der BauID GmbH ab.

Der Arbeitnehmer erhält eine BauID-Karte ausgestellt, diese kann, sofern eine aufrechte Nutzungsvereinbarung besteht, auf dem Bauvorhaben verwendet werden.

Sowohl die Baustellenverantwortlichen (auf vertraglicher Grundlage) als auch die Kontrollbehörden (auf gesetzlicher Grundlage), können durch die Nutzung der BauID schnell und verlässlich überprüfen, ob die auf der Baustelle tätigen Arbeitnehmer über die erforderlichen Erlaubnisse verfügen und, ob die gesetzlichen Meldeverpflichtungen (gegenüber ZKO, BUAK und OEGK) eingehalten wurden.

In weiterer Folge erfolgt die Nutzung wie folgt: Die Baustellen werden im BauID-System vom Generalunternehmer (Arbeitgeber) angelegt. Die einzelnen auf der Baustelle tätigen Unternehmen (einschließlich Subunternehmer) werden vom Generalunternehmen der jeweiligen Baustelle zugewiesen. Die Arbeitgeber weisen ihre Arbeitnehmer den jeweiligen Baustellen zu. Zu den Arbeitnehmern können die jeweiligen Arbeitgeber Dokumente hochladen.

Die **Kontrollbehörden** (Finanzpolizei, BUAK und ÖGK) können zur Erfüllung ihrer gesetzlichen Prüfpflichten die Kontrolle auf dem Bauvorhaben durch Verwendung der BauID-Karte durchführen. In der KontrollApp erhalten sei Einsicht in die zu den Arbeitnehmern hinterlegten Unterlagen (uA die nach dem LSD-BG erforderlichen Dokumente bei Entsendebetrieben bzw grenzüberschreitender Überlassung), die Versicherungsdaten der Arbeitnehmer (Schnittstelle OEGK), die Meldungen an die BUAK (Schnittstelle BUAK), die bei der Finanzpolizei hinterlegten Daten (Schnittstelle ZKO).

Werden Unterlagen iSd LSD-BG im BauID-System hinterlegt, gelten diese als rechtmäßig bereitgehalten und haben die Arbeitnehmer ihre Bereithaltungspflicht damit erfüllt.

Ebenso erhält der Arbeitgeber Einsicht in die von den Schnittstellen bereitgestellten Daten und die zum Arbeitnehmer hinterlegten Unterlagen.

Unabhängig von der oben dargestellten Kontrollfunktion auf Bauvorhaben können sich Arbeitnehmer unter Verwendung ihrer Kartennummer im BUAK-Info-System registrieren und tagesaktuelle Informationen über ihre Ansprüche bei der BUAK (z. B. den Urlaubsanspruch) abrufen.

2.1.5. Zuständigkeiten iZm der Verarbeitung

2.1.5.1 Verantwortliche:

Nach **Art. 4 Z 7 DSGVO** ist **Verantwortlicher** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die **Zwecke und Mittel** der Verarbeitung personenbezogener Daten entscheidet. Maßgeblich ist dabei die tatsächliche Entscheidungsbefugnis.

Der **Zweck** der Verarbeitung beantwortet die Frage, warum personenbezogene Daten verarbeitet werden, etwa zur Verwaltung von Nutzerkonten, zur Erfüllung eines Nutzungsvertrags oder zur Bereitstellung einer Software für Arbeitgeber.

Die **Mittel** der Verarbeitung betreffen insbesondere Entscheidungen darüber, welche Kategorien personenbezogener Daten verarbeitet werden, wer auf diese Daten zugreifen darf, wie lange sie gespeichert werden und an welche Empfänger sie übermittelt werden.

Die BUAK ist laut der zugrundeliegenden rechtlichen Bestimmungen Betreiberin der BauID Software. In dieser Funktion entscheidet die BUAK über die Zwecke und wesentlichen Mittel der damit verbundenen Verarbeitung personenbezogener Daten. Die BauID GmbH verarbeitet die personenbezogenen Daten auf Grundlage der mit der BUAK geschlossenen Nutzungsvereinbarung ausschließlich nach deren dokumentierten Vorgaben/Weisungen. Die BauID GmbH ist daher datenschutzrechtlich als **Auftragsverarbeiterin** (siehe sogleich unter 2.1.5.3.) der BUAK im Sinne des Art. 4 Z 8 DSGVO anzusehen.

2.1.5.2 Kontaktdaten der Verantwortlichen:

Bauarbeiter Urlaubs- und Abfertigungskasse
Kliebergasse 1A
1050 Wien

E-Mail: office@bauid.at

2.1.5.3 Auftragsverarbeiter

Nach **Art. 4 Nr. 8 DSGVO** ist **Auftragsverarbeiter** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im **Auftrag des Verantwortlichen verarbeitet.**

Der Auftragsverarbeiter verfolgt keine eigenen Zwecke hinsichtlich der Datenverarbeitung und handelt ausschließlich auf dokumentierte Weisung des Verantwortlichen.

Die BUAK als Verantwortliche ist verpflichtet, ein Register über die bestehenden Auftragsverarbeiter zu führen und entsprechende Vereinbarungen abzuschließen um die Einhaltung der Datensicherheitsmaßnahmen zu gewährleisten.

Die Auftragsverarbeiter sind zur Führung eines Verzeichnisses über die Datenverarbeitung und die Erstellung von Risikoanalysen verpflichtet.

2.2 Daten, Prozesse und Unterstützung

2.2.1. Welche Daten werden im BauID-System verarbeitet?

2.2. 1.1 Kategorien von Personen

Von der Datenverarbeitung im BauID-System sind **folgende Kategorien von (natürlichen) Personen betroffen** (betroffene Personen iSd DSGVO) :

- (Sub-)Unternehmen (**Betriebsinhaber**, bei Gesellschaften: **vertretungsbefugte Personen**)
- **Arbeitnehmer** die dem Anwendungsbereich des BUAG unterliegen (Verwaltung)
- **Arbeitnehmer** die dem Anwendungsbereich des BUAG unterliegen (Baustellenabfrage)
- **Arbeitnehmer** der (Sub-)Unternehmen, die nicht dem BUAG unterliegen (Verwaltung)
- **Arbeitnehmer** der (Sub-)Unternehmen, die nicht dem BUAG unterliegen (Baustellenabfrage)
- **Arbeitnehmer** der BauID/BUAK (Verwaltung und IT)
- Dienstleister (bzw deren **Mitarbeiter**) der (Sub-)Unternehmen (zB IT)
- Behörden (**Zugriffsberechtigte Personen** bei zB Finanzamt/Finanzpolizei, OEGK)
- **Zugriffsberechtigte Personen**/**Prüfer** bei BUAK
- **Mitarbeiter** der Dienstleister der BauID/BUAK (zB IT)

2.2.1.2. Kategorien von personenbezogenen Daten

Die Daten (Datenarten), die verarbeitet werden, sind folgenden Kategorien zuzuordnen

2.2.1.2.1. Besondere Kategorien von Daten (Art 9 DSGVO)

- Biometrische Daten (Bildaufnahmen) der Arbeitnehmer
- Ethnische Herkunftsdaten (Aussehen) der Arbeitnehmer

Personenbezogene Daten, die besonderen Kategorien iSd Art 9 DSGVO zuzuordnen sind, werden entsprechend des Löschkonzepts gelöscht, sobald sie nicht mehr benötigt werden

(Anlage). Die absolute Löschfrist beläuft sich gemäß § 34e BUAB auf 5 Jahre. „Triggerpunkt“ für die Löschung ist jeweils die Beendigung der Vertragsbeziehung.

Die Verarbeitung von personenbezogenen Daten besonderer Kategorien erfolgt für Arbeitnehmer, für die eine BauID-Karte ausgestellt wird. Der **Zweck** der Verarbeitung ist die Ausstellung der BauID-Karte. Zur Rechtsgrundlage der Datenverarbeitung siehe sogleich unten unter Pkt. 3.1.2, sowie in der Folge die Feststellung der Identität des Arbeitnehmers auf dem Bauvorhaben.

Empfänger der besonderen Kategorien von Daten sind

- BauID-Kartendienstleister (Auftragsverarbeiter)
- Kontrollbehörden im Zuge der Kontrolle
- Arbeitgeber und Generalunternehmer im Zuge der Kontrolle

2.2.1.2.2. Sonstige personenbezogene Daten:

Gruppe der **Betroffenen:** Arbeitnehmer

1. Name
2. Vorname
3. Geburtsdatum
4. Staatsbürgerschaft
5. Anschrift
6. Mailadresse
7. Telefonnummer
8. Sozialversicherungsnummer
9. Sozialversicherungsträger (bei entsendetem Arbeitnehmer)
10. Staat des Sozialversicherungsträgers (bei entsendetem Arbeitnehmer)
11. Geschlecht
12. Beruf
13. BUAK-Identifikationsnummer (bei AN, die dem BUAG unterliegen)
14. Login-Daten

Die personenbezogenen Daten werden gemäß des geltenden Löschkonzepts gelöscht. Die absolute Löschfrist beläuft sich gemäß § 34e BUAG auf 5 Jahren nach letztmaliger Nutzung der BauID-Karte bzw nach Ablauf der Karte.

Die **Empfänger** von sonstigen personenbezogenen Daten sind:

- AMS (Prüfung Beschäftigungsbewilligung – Schnittstelle): Daten mit der Nr. 1,2,3,4
- BMI (Bereitstellung Foto – Schnittstelle): Daten mit der Nr. 1,2,3,4
- BUAK (Prüfung): Daten mit der Nr. 1-14
- Dienstleisterregister OEGK (Schnittstelle): Daten mit der Nr. Nr. 1,2,3,4
- Video-Identitätsprüfungsdienstleisters: Daten mit der Nr. Nr. 1,2,3,4
- BauID-Kartendienstleister: Daten mit der Nr. 1,2,3,4,5
- ZKO-Meldungen (Schnittstelle): Daten mit der Nr. 1,2,3,4

- IT-Dienstleister der BauID GmbH: Daten mit der Nr. 1-14
- Finanzamt: Daten mit der Nr. Nr. 1,2,3,4
- ÖGK (Prüfung der rechtmäßigen Meldung: Daten mit der Nr. Nr. 1,2,3,4)

2.2.1.2.3.1 Zugriffsberechtigungen

Folgende Personen sind für das BauID System (BackOffice) **zugriffsberechtigt**:

Innerhalb der BUAK:

- Abteilungsleitung Abteilung „BUAK Online-Services“
- Sachbearbeiter der Abteilung „BUAK Online-Services“
- Buchhaltung
- IT-Abteilung
- Baustellenprüfer (bei Kontrolle auf der Baustelle)

Folgenden Personen sind für hinsichtlich des Abrufens der Daten mittels BauID-Karte auf dem Bauvorhaben zugriffsberechtigt.

Amt für Betrugsbekämpfung:

- Baustellenprüfer (bei Kontrolle auf der Baustelle)

OEGK:

- Baustellenprüfer (bei Kontrolle auf der Baustelle)

Unternehmen:

(hinsichtlich der Daten der eigenen Arbeitnehmer und die Arbeitnehmer ihrer Subunternehmen nach Zuordnung der Arbeitnehmer zur jeweiligen Baustelle)

- Berechtige Personen

2.2.2. Mit Hilfe welcher Mittel erfolgt die Datenverarbeitung?

Die Datenverarbeitung erfolgt durch die

- Verwendung der BauID-Sofware, insb. durch die Verwaltung von Benutzerkonten mit Rollen- und Berechtigungskonzept, zur Speicherung von Mitarbeit- und Baustellendaten, sowie durch ein Dokumentenmanagement für hinterlegte Unterlagen etc.
- Verwendung einer BauID-Karte mit NFC-Chip zur eindeutigen Identifikation der Arbeitnehmer
- die Verwendung von Mobilen Apps für die Verwendung von Bauleitern und Kontrollbehörden, Dokumentenmanagement für hinterlegte Unterlagen etc.
- Verwendung von digitalen Schnittstellen zur Abrufung von tagesaktuellen Informationen
- Protokollierung von Karten-Scans und Zugriffen.

3. GRUNDLEGENDE PRINZIPIEN

3.1. Verhältnismäßigkeit und Notwendigkeit

3.1.1. Verarbeitungszwecke

Die **Zwecke** und Datenverarbeitung sowie die Art der verarbeiteten Daten sind in § 34b BUAG normiert. Es erfolgt keine über die gesetzlich normierten Zwecke hinausgehende Verarbeitung der Daten.

3.1.2. Rechtmäßigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfolgt auf folgender Grundlage:

- Vertrag oder Vertragsanbahnung (Art. 6 lit b DSGVO)
- Erfüllung von rechtlichen Verpflichtungen (Art 6 lit c DSGVO)
- Wahrnehmung einer Aufgabe im öffentlichen Interesse (Art 6 lit e DSGVO)

Rechtsgrundlage für die Verarbeitung besonderer Kategorien (biometrische Daten zur Identifizierung einer Person) personenbezogener Daten:

Die Verarbeitung besonderer Kategorien von Daten darf ausschließlich auf Grundlage der in Art 9 DSGVO taxativ aufgezählten Grundlagen erfolgen.

BUAG-pflichtige Arbeitnehmer:

- **Art 9 Abs 2 lit g DSGVO**, die Verarbeitung erfolgt aufgrund eines Gesetzes, aus Gründen eines erheblichen öffentlichen Interesses erforderlich.

Nicht-BUAG-pflichtige Arbeitnehmer:

- **Einwilligung gemäß Art 9 Abs 2 lit a** DSGVO (Einwilligung im Zuge des Abschlusses der Nutzungsvereinbarung)

Rechtsgrundlage für die Verarbeitung sonstiger personenbezogener Daten im BauID-System im Rahmen der Personalverwaltung der Nutzer der BauID (Unternehmen):

- Vertrag oder Vertragsanbahnung (Art. 6 lit b DSGVO)
- Wahrnehmung einer Aufgabe im öffentlichen Interesse (Art 6 lit e DSGVO)

Nach Beendigung der Vertragsbeziehung kann eine Verarbeitung erfolgen auf Grundlage von:

- Erfüllung von rechtlichen Verpflichtungen (Art 6 lit c DSGVO)

3.1.3. Sind die erhobenen Daten der Arbeitnehmer erforderlich, relevant und auf das für die Datenverarbeitung Notwendige beschränkt?

Zweck des BauID-Systems ist die Bekämpfung von Sozialbetrug, Lohn- und Sozialdumping und illegaler Beschäftigung sowie die Unterstützung der gesetzlich vorgesehenen Kontroll- und Nachweispflichten auf Baustellen. Darüber hinaus dient das System der effizienten Verwaltung von Arbeitnehmern, Baustellen und den hierfür erforderlichen Berechtigungen sowie der Erfüllung gesetzlicher Melde- und Dokumentationspflichten.

Die Verarbeitung personenbezogener Daten ist **erforderlich**, um die Identität der auf Baustellen eingesetzten Arbeitnehmer zuverlässig festzustellen, deren Berechtigungen und Meldestatus zu überprüfen sowie die gesetzlich vorgesehenen Kontrollen durch Arbeitgeber und zuständige Behörden effizient durchführen zu können. Ohne die Verarbeitung der im BauID-System

vorgesehenen Daten könnten die gesetzlichen Aufgaben nicht oder nur mit einem unverhältnismäßig hohen organisatorischen und administrativen Aufwand erfüllt werden.

Die **Verarbeitung besonderer Kategorien personenbezogener Daten** beschränkt sich auf jene Daten, die für die Ausstellung der BauID-Karte und die zuverlässige Identitätsfeststellung erforderlich sind. Eine Verarbeitung erfolgt ausschließlich, soweit hierfür eine gesetzliche Grundlage oder – soweit gesetzlich vorgesehen – eine wirksame Einwilligung besteht.

Die im BauID-System verarbeiteten personenbezogenen Daten sind auf das zur Erreichung der festgelegten Verarbeitungszwecke erforderliche Maß beschränkt (Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO).

Es werden ausschließlich jene Daten verarbeitet, die für die Identifizierung der Arbeitnehmer, die Zuordnung zu Bauvorhaben, die Erfüllung gesetzlicher Melde-, Nachweis- und Kontrollpflichten sowie die Ausstellung und Nutzung der BauID-Karte erforderlich sind. Besondere Kategorien personenbezogener Daten werden nur verarbeitet, soweit dies für die Ausstellung der BauID-Karte oder aufgrund einer gesetzlichen Verpflichtung erforderlich ist.

Eine Verarbeitung zusätzlicher personenbezogener Daten, die für diese Zwecke nicht erforderlich sind, erfolgt nicht. Die einzelnen Datenkategorien wurden im Vorfeld hinsichtlich ihrer Erforderlichkeit geprüft. Kann ein Verarbeitungszweck mit weniger oder weniger eingriffsintensiven personenbezogenen Daten erreicht werden, wird auf die Verarbeitung darüberhinausgehender Daten verzichtet.

Durch Rollen- und Berechtigungskonzepte sowie eine zweckgebundene Datenverarbeitung wird sichergestellt, dass nur jene Personen Zugriff auf personenbezogene Daten erhalten, die diese zur Erfüllung ihrer gesetzlichen oder vertraglichen Aufgaben benötigen. Damit wird gewährleistet, dass die Verarbeitung insgesamt erforderlich und verhältnismäßig erfolgt.

3.1.4. Sind die Daten korrekt und auf dem neuesten Stand?

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden ("Richtigkeit").

Die Betroffenen können ihr Recht auf **Berichtigung** unter [office@bauid.at] oder postalisch oder persönlich gegenüber der BUAK geltend machen. Die Information über die Betroffenenrechte erfolgt bei Registrierung der Arbeitnehmer und ist auf der Homepage der BauID jederzeit abrufbar.

Im Hinblick auf die Datenquellen sind die führenden Systeme festgelegt. Durch etablierte Prozesse (zB Statistiken, Einsicht in die Register) wird die Datenqualität regelmäßig überprüft.

3.1.5. Für welche Dauer werden die Daten gespeichert?

Die Daten werden gespeichert, solange die Speicherung für die Zweckerreichung notwendig ist.

Hinsichtlich der Datennutzung wurde ein Löschkonzept erstellt. Darüber hinaus ist eine gesetzliche absolute Löschfrist von 5 Jahren bzw hinsichtlich der Scandaten von 3 Jahren normiert. Auslöser der Löschfrist ist jeweils das Ende der vertraglichen Beziehung (Ablauf der Nutzerpakete).

Die Betroffenen haben nach DSGVO das Recht, jederzeit die Löschung ihrer Daten zu beantragen. Auf dieses Recht und die Form der Geltendmachung wird in der DSGVO-Information ausdrücklich hingewiesen.

3.2. Maßnahmen zum Schutz der Persönlichkeitsrechte der betroffenen Personen

3.2.1. Wie werden die betroffenen Personen über die Verarbeitung informiert?

Den Informationspflichten wird derzeit mittels eines Informationsformulars nachgekommen, welches auf der Web-Seite der BauID [*www.bauid.at/Datenschutz]* unter dem Punkt Datenschutzerklärung/Informationspflichten abrufbar ist. Die Kenntnisnahme der Datenschutzinformation ist zu bestätigen.

Im Informationsformular sind die Informationen gemäß Art 13 und 14 DSGVO zur Verarbeitung personenbezogener Daten durch die BauID-Software enthalten. Dieses enthält folgende Angaben:

- Name und Kontaktdaten des Verantwortlichen
- Person des Datenschutzbeauftragten
- Zweck der Verarbeitung
- Rechtsgrundlage
- Datenkategorien
- Personenkategorien
- Empfängerkategorien
- Fristen für die Löschung
- Rechte der betroffenen Personen
- Beschwerderecht

3.2.2. Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt?

Die Einwilligung der Personen wird vor Ausstellung der BauID-Karte eingeholt. Sie erfolgt schriftlich mittels vorgefertigten Formulars.

3.2.3. Wie können Betroffene ihre Rechte ausüben?

Das Recht auf Auskunft, Berichtigung, Einschränkung, Widerspruch und Datenübertragbarkeit kann **via E-Mail** unter (office@bauid.at), **postalisch**, **persönlich** oder **telefonisch** geltend gemacht werden.

3.2.4 Sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?

Mit den Auftragsverarbeitern werden Auftragsverarbeitungsverträge iSd DSGVO abgeschlossen. Diese enthalten klare Verpflichtungen und Vorgaben für die Verarbeitung der personenbezogenen Daten. Alle Auftragsverarbeiter sind in einem Verzeichnis zu erfassen. Die Auftragsverarbeitungsverträge sind von der BUAK zu dokumentieren.

3.2.5 Soweit Datenübermittlungen in Länder außerhalb der Europäischen Union stattfinden, werden die Daten angemessen geschützt?

Die Übermittlung der personenbezogenen Daten an ein Drittland oder eine internationale Organisation findet **nicht** statt.

4. BESTEHENDE MAßNAHMEN ZUR DATENSICHERHEIT

Die BUAK hat im Rahmen des Betriebs des BauID-Systems zahlreiche technische und organisatorische Maßnahmen zum Schutz der Datensicherheit (TOMs) etabliert. Diese umfassen insbesondere Maßnahmen in den folgenden Bereichen:

- Verschlüsselung,
- Zugriffskontrolle,
- Datentrennung,
- Protokollierung,
- Archivierung und Datenminimierung,
- Betriebssicherheit,
- Datensicherung,
- Netzwerksicherheit,
- Hardware- und Zugangssicherheit,
- Datenschutzorganisation,
- Datenschutzrichtlinien,
- Risikomanagement,
- Sensibilisierung der Mitarbeitenden

Die detaillierten technischen und organisatorischen Maßnahmen (TOMs) sind aus Sicherheitsgründen in dieser zusammenfassenden Version nicht enthalten. Alle TOMs sind dokumentiert und werden der Datenschutzbehörde im Bedarfsfall bzw. auf Verlangen offengelegt.

5. RISIKEN UND RISIKOBEWERTUNG

5.1 Risiko: Unrechtmäßiger Zugriff auf Daten (lesend oder schreibend)

5.1.1 Was könnten die wesentlichen Auswirkungen für die betroffenen Personen (Arbeitnehmer) sein, wenn das Risiko eintritt?

- Offenlegung besonderer Kategorien personenbezogener Daten (biometrische Daten, insbesondere Gesichtsprofile) durch Datendiebstahl oder unbefugten Zugriff,
- Offenlegung personenbezogener Daten (z. B. Stammdaten, Wohnsitz, Geburtsdatum, Arbeitszeiten) durch Datendiebstahl oder unbefugten Zugriff,
- Identitätsmissbrauch oder missbräuchliche Verwendung personenbezogener Daten,
- Verlust der Kontrolle über biometrische Daten, die im Gegensatz zu Passwörtern nicht ohne Weiteres geändert werden können,
- Gefährdung des Arbeitsplatzes und damit des Einkommens des Arbeitnehmers durch unrechtmäßige Löschung oder Manipulation arbeitsrelevanter Dokumente,

- DSGVO-widrige Verarbeitung von Fotos und Dokumenten, insbesondere bei Diebstahl oder Fälschung der entsprechenden Einwilligungen,
- Bürokratischer Aufwand durch die neuerliche Beschaffung von Daten und Dokumenten,
- Missbräuchliche Weitergabe oder der Verkauf personenbezogener Daten,
- Verwendung der Daten für andere als die vorgesehenen Zwecke

5.1.2 Was sind die Hauptbedrohungen, die zu dem Risiko (unrechtmäßiger Zugriff auf Daten) führen könnten?

- Zugriff durch unbefugte Mitarbeiter der (Sub-)Unternehmen,
- Zugriff durch unbefugte Mitarbeiter der BUAK,
- Diebstahl der Zugangsdaten durch Dritte,
- Zugriff auf die Daten durch Cyberangriffe

5.1.3 Was sind die Risikoquellen?

- Mitarbeiter, der Zugangsdaten vorsätzlich missbraucht,
- Mitarbeiter, die ihre Zugangsdaten nicht ausreichend schützen,
- Mitarbeiter, die Zugangsdaten an Nichtbefugte weitergeben,
- Fehler bei der Benutzung des Systems durch Mitarbeiter durch mangelnde Schulung oder fehlendes Sicherheitsbewusstsein,
- Datenspionage durch Mitarbeiter,
- Unbefugte Dritte, die auf die Daten zugreifen
- Angreifer, die berechtigte Nutzer zur Preisgabe ihrer Zugangsdaten verleiten (z. B. Phishing oder Social Engineering).
- Cyberangreifer,
- Eine dritte Partei, die ihren autorisierten Zugang zweckwidrig nutzt

5.1.4 Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos (unrechtmäßiger Zugriff auf Daten) bei?

- Logische Zugriffskontrolle,
- Zugangskontrolle,
- Datentrennung,
- Datensicherungen,
- Bekämpfung von Malware,
- Netzwerksicherheit,
- Zugangskontrolle,
- Überwachen der Netzwerkaktivität,
- Verschlüsselung,
- Rückverfolgbarkeit (Protokollierung),
- Betriebssicherheit,
- Arbeitsplatzverwaltung,
- Schutz des Internetauftritts

5.1.5 Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Ohne die Umsetzung der geplanten Maßnahmen wäre wohl von einem *hohen Risikoschweregrad* auszugehen.

Ein unrechtmäßiger Zugriff auf personenbezogene Daten könnte zu erheblichen Beeinträchtigungen der Rechte und Freiheiten der betroffenen Personen führen. Insbesondere könnten sensible personenbezogene Daten offengelegt oder missbräuchlich verwendet werden. Darüber hinaus könnten unrechtmäßige Löschungen oder Veränderungen arbeitsrelevanter Dokumente zu Nachteilen für die betroffenen Arbeitnehmer sowie zu Beeinträchtigungen der gesetzlichen Prüf- und Dokumentationspflichten der Arbeitgeber und der Kontrolltätigkeit der BUAK führen.

Bei ordnungsgemäßer Umsetzung der vorgesehenen technischen und organisatorischen Maßnahmen wird das verbleibende *Restrisiko als niedrig und vertretbar* eingeschätzt.

5.1.6 Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos (unrechtmäßiger Zugriff auf Daten) ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Ohne die geplanten Sicherheitsmaßnahmen wäre eine *hohe Eintrittswahrscheinlichkeit* nicht auszuschließen.

Nach ordentlicher Umsetzung der geplanten Maßnahmen wir die Eintrittswahrscheinlichkeit als *niedrig* eingeschätzt.

5.2 Risiko: Unerwünschte Veränderung von Daten

5.2.1 Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

- Fehlerhafte oder missbräuchliche Leistungsabrechnung,
- Nachteile aufgrund unrichtiger oder unvollständiger personenbezogener Daten,
- Verzögerungen und Beeinträchtigungen bei Prüfverfahren durch die Kontrollbehörden,
- DSGVO-widrige Verarbeitung von Fotos und Dokumenten,
- Bürokratischer Aufwand durch Korrektur der Daten,
- Gefährdung des Arbeitsplatzes oder finanzieller Ansprüche infolge fehlerhafter Daten

5.2.2 Was sind die Hauptbedrohungen, die zu dem Risikon (unerwünschte Veränderung von Daten) führen könnten?

- Veränderung durch Mitarbeiter der (Sub-)Unternehmen,
- Veränderung durch Mitarbeiter der BUAK,
- Veränderung durch Diebstahl der Zugangsdaten
- Veränderung durch Diebstahl der Hardware,
- Veränderung durch Cyberangriffe

5.2.3. Was sind die Risikoquellen?

- Vorsätzliches Handeln von Mitarbeitern,
- Nachlässiges Handeln von Mitarbeitern,
- Fehler bei der Nutzung des Systems,
- Vorsätzliches Handeln Dritter,
- Dritte, die einen autorisierten Zugang zweckwidrig verwenden,
- Cyberangreifer,
- Ausfälle des Systems, Stromausfall, Feuer, Naturkatastrophen, Überschwemmungen

5.2.4 Welche Maßnahmen tragen zur Bewältigung des Risikos (unerwünschte Veränderungen von Daten) bei?

- Logische Zugriffskontrollen,
- Datentrennung,
- Rückverfolgbarkeit (Protokollierung),
- Betriebssicherheit,
- Datensicherungen,
- Hardware- und Gerätewartung,
- Arbeitsplatzverwaltung,
- Bekämpfung von Malware,
- Netzwerksicherheit,
- Schutz des Internetauftritts,
- Verschlüsselung von Daten

5.2.5 Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Ohne Umsetzung der geplanten Maßnahmen wäre von einem *hohen Risikoschweregrad* auszugehen.

Eine unrechtmäßige Veränderung personenbezogener Daten kann zu erheblichen Nachteilen für die betroffenen Personen führen. Darüber hinaus können dadurch gesetzliche Prüf- und Dokumentationspflichten der Arbeitgeber beeinträchtigt sowie Prüfverfahren der BUAK verfälscht oder erschwert werden.

Bei ordnungsgemäßer Umsetzung der vorgesehenen technischen und organisatorischen Maßnahmen wird das verbleibende *Restrisiko als niedrig und vertretbar* eingeschätzt.

5.2.6 Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?

Ohne die geplanten Maßnahmen würde eine *hohe Eintrittswahrscheinlichkeit* vorliegen.

Bei Umsetzung der geplanten Maßnahmen wird die Eintrittswahrscheinlichkeit als *niedrig* eingeschätzt.

5.3 Risiko: Datenverlust

5.3.1. Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko (Datenverlust) eintritt?

- Verlust personenbezogener Daten und arbeitsrelevanter Dokumente,
- Gefährdung des Arbeitsplatzes und damit des Einkommens des Arbeitnehmers,
- DSGVO-widrige Verarbeitung von Fotos und Dokumenten, insbesondere bei Verlust der entsprechenden Einwilligungen,
- Bürokratischer Aufwand durch die neuerliche Beschaffung der Daten und Dokumente,
- Nachteile bei der Geltendmachung arbeits- oder sozialrechtlicher Ansprüche

5.3.2. Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

- Löschung durch Mitarbeiter,
- Löschung durch Dritte,
- Löschung infolge Systemfehlern,

- Löschung infolge Cyberangriffe

5.3.3 Was sind die Risikoquellen?

- Böswillige Mitarbeiter,
- Nachlässige Mitarbeiter,
- Böswillige Dritte,
- Angreifer, die berechtigte Nutzer zur Durchführung schädlicher Handlungen verleiten,
- Cyberangreifer,
- Dritte, die ihren autorisierten Zugang zweckwidrig verwenden,
- Systemausfälle, Stromausfälle, Feuer, Naturkatastrophen oder Überschwemmungen

5.3.4. Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

- Datensicherung,
- Wiederherstellungstest,
- Notfallmanagement,
- Rückverfolgbarkeit (Protokollierung),
- Betriebssicherheit,
- Datensicherungen,
- Hardware-/Gerätewartung,
- Bekämpfung von Malware,
- Netzwerksicherheit,
- Hardware-Sicherheit,
- Zugangskontrolle,
- Überwachen der Netzwerkaktivität

5.3.5. Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Ohne die geplanten Maßnahmen würde ein *hoher Risikoschweregrad* vorliegen.

Bei Umsetzung der technischen und organisatorischen Maßnahmen wird das verbleibende Restrisiko als *niedrig* bzw. *vertretbar* eingeschätzt.

5.3.6. Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?

Ohne die geplanten Maßnahmen würde eine *hohe* Eintrittswahrscheinlichkeit vorliegen

Bei Umsetzung der geplanten Maßnahmen ist die Eintrittswahrscheinlichkeit als *niedrig* einzuschätzen.

6. WEITERE SCHRITTE

Nach **Art 36 Abs 1 DSGVO** ist vor der Verarbeitung die Aufsichtsbehörde zu konsultieren, wenn die Verarbeitung ein hohes Risiko zur Folge hat und der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Da die Risikobewertung unter Berücksichtigung der gesetzten Maßnahmen ergeben hat, dass insgesamt für die Rechte und Freiheiten der Betroffenen überschaubare Risiken bestehen, ist dieser Schritt nicht erforderlich.

BAUID

DEIN
DIGITALER
SERVICE
AM BAU