Datenschutzreglement

Art. 1 Zweckbestimmung

Der Paritätische Verein «Informationssystem Allianz Bau» (ISAB) betreibt eine Datenbanklösung.

Paritätische Kommissionen, Kontrollvereine und Betriebe verwalten Daten auf dem Informationssystem Allianz Bau. Sie beauftragen ISAB mit der Durchführung entsprechender Prozesse wie die Ausgabe von GAV-Bescheinigungen oder der Herstellung eines Ausweises für Mitarbeitende von GAV unterstellten Firmen (ISAB-Card) und dessen Online-Abfrage mittels einer ISAB Kontroll-Applikation (ISAB-App).

Ausführungsbestimmungen zu diesem Reglement finden sich in den Datenbearbeitungsgrundsätzen ISAB. Diese bilden den Anhang 1 zu diesem Reglement.

Art. 2 Verantwortlichkeit für Datenbearbeitung

Jede Bearbeitung von Daten natürlicher oder juristischer Personen durch den Verein ISAB erfolgt in seiner Rolle als Auftragsbearbeiter. Die Verantwortung für den Inhalt der Daten liegt bei den Paritätischen Kommissionen, den Kontrollvereinen und den Betrieben.

Art. 3 Nutzungsvereinbarung und AGB

Der Verein ISAB schliesst mit den Paritätischen Kommissionen und den Kontrollvereinen, die Daten auf das System einliefern, eine Nutzungsvereinbarung ab. Die Betriebe, welche Daten auf der ISAB-Plattform erfassen und GAV-Bescheinigungen oder ISAB-Cards bestellen, unterzeichnen Allgemeine Geschäftsbedingungen (AGB).

Art. 4 Erstellen von User-Berechtigungen

Wenn eine Paritätische Kommission, ein Kontrollverein, eine Vergabestelle oder ein Betrieb die Nutzungsvereinbarung oder die AGB unterzeichnet hat, erhält sie einen Zugang zum Informationssystem Allianz Bau. Damit kann sie User-Berechtigungen selbst eröffnen und verwalten.

Ohne unterzeichnete Nutzungsvereinbarung oder AGB dürfen keine User angelegt werden.

Nicht als Dritte gelten die ISAB-Organe und die ISAB-Geschäftsstelle mit ihren Mitarbeiterinnen und Mitarbeitern sowie die von ISAB beauftragten IT-Dienstleister für Entwicklung und Wartung der ISAB-Datenbank. Diese ISAB internen Berechtigungen werden nur solange und soweit vergeben, als sie zur Erfüllung der Aufgaben einer Person notwendig sind.

Art. 5 User-Verwaltung

Auf ISAB dürfen nur persönliche User eingerichtet werden. Benutzer/innen, die eine User-Berechtigung erhalten, sind zur Vertraulichkeit und zur Einhaltung der Datenschutzbestimmungen und allen anderen Vorgaben verpflichtet.

Paritätische Kommissionen, Kontrollvereine, Vergabestellen und Betriebe, die Berechtigungen auf dem Informationssystem Allianz Bau verwalten, sind für die entsprechende Instruktion der von ihr erfassten User verantwortlich. Zudem sind sie dafür verantwortlich, dass die User-Berechtigungen desaktiviert werden, wenn ein User sie nicht mehr benötigt.

Auf Verlangen des Vereins ISAB müssen sie Rechenschaft über die erfassten User ablegen und nachweisen, dass die entsprechenden Instruktionen erfolgt sind.

Die Geschäftsstelle ISAB regelt die Verwendung der internen ISAB-Userberechtigungen.

Art. 6 Aufzeichnung

Alle Datenänderungen auf dem Informationssystem Allianz Bau werden protokolliert, insbesondere auch die Abfrage einer GAV-Bestätigung, die Bestellung von ISAB-Cards sowie deren Abfrage.

Der Verein ISAB überwacht das System aktiv und führt eine Aufzeichnung der Sicherheitsverletzungen mit einer Beschreibung des Verstosses, des Zeitraums, der Folgen des Verstosses, des Namens des Berichterstatters und an wen der Verstoss gemeldet wurde, und des Verfahrens zur Wiederherstellung der Daten.

Der Verein ISAB stellt den Paritätischen Kommissionen, Kontrollvereinen und Betriebe Auswertungen zu den Datenänderungen in ihrem Verantwortungsbereich zur Verfügung.

Auf Verlangen stellt der Verein ISAB zudem benutzerbezogene Auswertungen zur Verfügung.

Art. 7 Überprüfung der eingesetzten technischen Mittel und der Datensicherheit

Der Verein ISAB überprüft periodisch, mindestens einmal jährlich, zusammen mit einer geeigneten IT-Unternehmung, ob die technischen Voraussetzungen weiterhin ausreichen, um einen angemessenen Datenschutz zu gewährleisten, insbesondere

- technische Fehler und zufällige Verluste oder Vernichtung der ganzen Sammlung zu minimieren;
- unbefugte Eingriffe in die Sammlung und unbefugten Zugriff zu verhindern;
- zu überprüfen, ob die eingesetzten Systeme dem aktuellen Stand der Technik entsprechen.

Über den Audit und allfällige Empfehlungen wird ein Protokoll erstellt.

Art. 8 Auskunftsbegehren

Die Paritätischen Kommissionen und Kontrollvereine, welche eine Nutzungsvereinbarung unterzeichnet haben, beauftragen den Verein ISAB, Auskunftsbegehren gemäss Datenschutzgesetz in ihrem Namen zu bearbeiten. Die Einzelheiten sind in den entsprechenden Verträgen geregelt.

Wer Auskunft über die über ihn gespeicherten Daten gemäss Datenschutzgesetz verlangt, hat sich darüber zu erklären, ob er

- als Privatperson oder
- als bevollmächtigter Vertreter einer juristischen Person

Auskunft wünscht.

Gesuchsteller haben sich durch geeignete Dokumente über ihre Identität auszuweisen und eine genügend unterzeichnete Vollmacht der juristischen Person vorzuweisen, soweit sich die Legitimation, für diese zu handeln, nicht eindeutig aus dem Handelsregister bereits ergibt.

Ist die Identität nachgewiesen, erteilt der Verein ISAB Auskunft und informiert die zuständigen Paritätischen Kommissionen und Kontrollvereine.

Ist die Identität nachgewiesen und bezieht sich das Auskunftsbegehren auf Mitarbeiterdaten, die von Betrieben verwaltet werden, verweist ISAB die auskunftsersuchende Person an den oder die zuständigen Betriebe.

Art. 9 Berichtigungsbegehren

Wird ein Begehren um Berichtigung oder Löschung eines Eintrages gestellt, wird vom Verein ISAB umgehend ein entsprechender Vermerk in der Datenbank angebracht und das Begehren an die zuständigen Paritätischen Kommissionen, Kontrollvereine und Betriebe weitergeleitet, die das weitere Verfahren selber führen.

Art. 10 Inkrafttreten und Änderungen

Dieses Reglement und der Anhang «Datenbearbeitungsgrundsätze ISAB» wurden von der Mitgliederversammlung des Vereins «Informationssystem Allianz Bau» am 27.2.2019 genehmigt und mit sofortiger Wirkung in Kraft gesetzt.

Anhang zum Datenschutzreglement ISAB: Datenbearbeitungsgrundsätze ISAB

ISAB verpflichtet sich und gewährleistet gegenüber Vertragspartnern, die mit ihr eine Nutzungsvereinbarung abschliessen:

1 Datenschutz

a) die Personendaten nur für die Zwecke des Vertragspartners zu verarbeiten, und jeweils nur zum Zwecke der Durchführung der Nutzungsvereinbarung oder der AGB, gemäss den dokumentierten Instruktionen des Vertragspartners. Hierzu vereinbart ISAB mit dem Vertragspartner, dass die Ausgestaltung der Dienstleistung gemäss Nutzungsvereinbarung und derer im Rahmen der Dienstleistung vorgesehenen Konfiguration und Steuerung durch den Vertragspartner die abschliessenden, verbindlichen Instruktionen des Vertragspartners darstellen. Sind weitere Instruktionen erforderlich und können diese vom Anbieter nicht im Rahmen seiner Ressourcen und zur Verfügung gestellten Ressourcen umgesetzt werden, so wird der Vertragspartner die Instruktionen entsprechend modifizieren oder die Nutzungsvereinbarung kündigen.

b) keine Personendaten (auch nicht im Zusammenhang mit einer Bearbeitung von Personendaten, die im Rahmen der betreffenden bestehenden Vereinbarung erlaubt ist) zu exportieren ohne dass dafür eine vertragliche Grundlage besteht;

c) geeignete technische und organisatorische Massnahmen vorzusehen und aufrechtzuerhalten, um eine unbefugte Bearbeitung, den Verlust oder die Beschädigung von Personendaten zu verhindern, insbesondere die unten unter Ziff. 2 genannten Massnahmen;

d) sich bei der Bearbeitung von Personendaten nur auf Mitarbeiter und sonstige Hilfspersonen zu verlassen, die vertraglich oder gesetzlich zur Verschwiegenheit verpflichtet sind, wobei ISAB für das Verhalten seiner Mitarbeiter und sonstigen Hilfspersonen wie für sein eigenes Verhalten verantwortlich bleibt;

e) die Bearbeitung von Personendaten an einen Dritten (ausser Mitarbeitern und anderen Hilfspersonen, die die Anforderungen von Absatz (d) erfüllen) nur mit vorheriger schriftlicher Zustimmung des Vertragspartners zu delegieren und nur an einen Unterauftragsbearbeiter, der verpflichtet ist, Bestimmungen über Vertraulichkeit und Datenschutz einzuhalten, die mindestens ebenso streng sind, wie die Bestimmungen der Nutzungsvereinbarung, des Datenschutzreglements und dieser Datenverarbeitungsgrundsätze und weiter gilt, dass ISAB für das Verhalten eines seiner Unterauftragsbearbeiter wie für sein eigenes Verhalten verantwortlich bleibt; die Zustimmung gilt ferner als erteilt für Unterauftragsbearbeiter, die dem Vertragspartner mindestens 30 Tage im Voraus vom Anbieter in Textform mitgeteilt werden; vorausgesetzt jedoch, dass wenn der Vertragspartner dem vorgesehenen Unterauftragsbearbeiter innerhalb von 30 Tagen nach Erhalt der Mitteilung widerspricht, ISAB die Bearbeitung von Personendaten nicht an diesen Unterauftragsbearbeiter delegieren darf; in diesem Fall darf ISAB jedoch die Nutzungsvereinbarung mit einer Frist von drei Monaten kündigen;

f) unverzüglich dem Vertragspartner (i) jede tatsächliche oder vermutete Datenschutzverletzung zusammen mit allen Informationen gemäss Artikel 33 Absatz 3 DSGVO und sonst anwendbaren Datenschutzvorschriften, die ISAB zur Verfügung stehen, zu melden, (ii) jede tatsächliche oder

drohende Beeinträchtigung oder Unzulänglichkeit von ISAB in der Erfüllung einer der Bestimmungen der Nutzungsvereinbarung, des Datenschutzreglements oder diesen Datenbearbeitungsgrundsätzen zu melden, und (iii) jeden Antrag auf Zugriff auf Personendaten und jeden tatsächlichen Zugriff auf Personendaten durch Behörden zu melden, es sei denn, gesetzliche Vorgaben verbieten die Meldung aus wichtigen Gründen des öffentlichen Interesses;

g) auf Anfrage des Vertragspartners, den Vertragspartner bei der Einhaltung der anwendbaren Datenschutzvorschriften auf die gewünschte Art und Weise zu unterstützen (einschliesslich, aber nicht beschränkt auf, den Vertragspartner bei der Erfüllung seiner Verpflichtungen zu unterstützen, (i) den betroffenen Personen zu antworten, die ihre Rechte gemäss den anwendbaren Datenschutzvorschriften, einschliesslich Kapitel III der DSGVO, ausüben, und (ii) den Anforderungen der Artikel 32 bis 36 DSGVO und entsprechender Bestimmungen anderer anwendbarer Datenschutzvorschriften nachzukommen, unter Berücksichtigung der Art der Bearbeitung und der ISAB zur Verfügung stehenden Informationen). Der Vertragspartner erstattet ISAB angemessene Kosten und Auslagen, die ISAB bei der Unterstützung des Vertragspartners gemäss diesem Abschnitt entstanden sind;

h) den Vertragspartner unverzüglich zu informieren, falls eine Instruktion des Vertragspartners an ISAB betreffend Bearbeitung der Personendaten voraussichtlich anwendbare datenschutzrechtliche oder andere anwendbare Bestimmungen verletzen könnte;

i) dem Vertragspartner alle Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung dieses Artikels 3 durch ISAB nachzuweisen und Inspektionen zu erlauben und zu unterstützen, einschliesslich Inspektionen durch den Vertragspartner oder einen anderen vom Vertragspartner beauftragten Prüfer, vorbehaltlich der üblichen Vertraulichkeitsvereinbarungen. Darüber hinaus muss ISAB dem Vertragspartner jeden Auditbericht zur Verfügung stellen, der vom Prüfer von ISAB erstellt wurde und die Einhaltung des Artikels 3 durch ISAB betrifft; und

j) vorbehaltlich der anwendbaren gesetzlichen Aufbewahrungspflichten, nach Beendigung der Nutzungsvereinbarung oder auf Anfrage des Vertragspartners, die Personendaten an den Vertragspartner zurückzugeben oder zu löschen, ohne eine Kopie aufzubewahren, und die Löschung dem Vertragspartner zu bestätigen.

2 Datenbearbeitungsgrundsätze der Anbieterin gegenüber Betrieben

Die Anbieterin gewährleistet eine datenschutzkonforme Information der Betriebe, welche auf der Plattform ISAB erfasst sind. Die Anbieterin gewährleistet, dass GAV-Bescheinigungen von Betrieben, welche Bauherren und Vergabestellen keine Informationen zur Verfügung stellen wollen, als gesperrt gekennzeichnet werden.

3 Technische und organisatorische Massnahmen

Anforderung: Verhindern, dass Unbefugte Zugang zu Daten-Bearbeitungssystemen erhalten, auf denen Personendaten bearbeitet werden:

Die physische Zugangskontrolle wird durch geeignete Massnahmen sichergestellt. Die Räumlichkeiten werden mit den üblichen Massnahmen verschlossen. Die Systeme des Anbieters sind durch geeignete physische Zugangskontrollen geschützt. Für Systeme, die bei externen Dienstleistern untergebracht, gehostet und gewartet werden, hat ISAB entsprechende Massnahmen veranlasst, die von diesen Dienstleistern umgesetzt und aufrechterhalten werden, darunter Zugangskontrollen mit Protokollierung, Richtlinien zur Überwachung und Identifikation der Gäste im Gebäude und Videoüberwachung an allen Ein- und Ausgängen.

Anforderung: Verhindern, dass Daten-Bearbeitungssysteme von Unbefugten eingesehen, kopiert, verändert oder gelöscht werden:

ISAB stellt die elektronische Zugangskontrolle durch geeignete Massnahmen sicher. Insbesondere ist der Zugang zu den Daten-Bearbeitungssystemen passwortgeschützt und wird nur autorisierten Personen gewährt, die zur Vertraulichkeit und zur Einhaltung der Datenschutzbestimmungen verpflichtet sind. ISAB hat geeignete Verschlüsselungsmethoden implementiert und verwendet geeignete Anti-Malware- und Anti-Virus-Kontrollen, um zu verhindern, dass schädliche Software unbefugten Zugriff auf Personendaten erhält. ISAB führt ein Verzeichnis der Datenträger, auf denen Personendaten bearbeitet werden. ISAB verwendet eine intelligent strukturierte Vergabe von Berechtigungen und stellt sicher, dass Berechtigungen für den Datenzugriff nur an Personen vergeben werden, die einen Bedarf haben und autorisiert sind, darauf zuzugreifen. ISAB stellt sicher, dass Personen, die zur Nutzung eines Daten-Bearbeitungssystems berechtigt sind, nur Zugang zu den Daten haben, die unter ihre Zugangsberechtigung fallen, und dass Personendaten während der Bearbeitung oder Nutzung oder nach der Speicherung nicht von Unbefugten eingesehen, gelesen, kopiert, verändert oder entfernt werden können.

Anforderung: Sicherstellen, dass bei der elektronischen Übermittlung oder während des Transports oder der Speicherung auf einem Datenträger Personendaten nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen Personendaten durch Datenübertragungseinrichtungen übermittelt werden sollen:

ISAB stellt die Übertragungskontrolle durch geeignete Massnahmen sicher, insbesondere durch eine verschlüsselte Verbindung für den Datenzugriff und die Datenübertragung über öffentliche Netzwerke. Die Datenübertragung über das Internet ist nur dort vorgesehen, wo es zur Erfüllung der Aufgaben des Anbieters unbedingt erforderlich ist. Die Daten werden nur dann auf tragbaren Datenträgern gespeichert, wenn es unbedingt notwendig ist, um die Aufgaben des Anbieters zu erfüllen. Wenn dem so ist, wird eine entsprechende Verschlüsselung angewendet. Eine Weitergabe der Daten an unbekannte Dritte findet nicht statt. ISAB trifft geeignete Massnahmen, um die Entfernung von Personendaten aus seinen Systemen nach Beendigung der jeweiligen Bestehenden Vereinbarung sicherzustellen.

Anforderung: Sicherstellen, dass überprüft und festgestellt werden kann, ob und von wem Personendaten in Daten-Bearbeitungssysteme eingegeben, geändert oder entfernt wurden:

ISAB stellt die Eingabekontrolle durch geeignete Massnahmen sicher. Insbesondere wird dokumentiert, wer wann Daten erfassen oder ändern kann. Die vorherige Version kann bei Bedarf jederzeit wiederhergestellt werden. Datenänderungen werden protokolliert, insbesondere auch die Abfrage einer GAV-Bestätigung, die Bestellung von ISAB-Cards sowie deren Abfrage[1]. ISAB führt eine Aufzeichnung der Sicherheitsverletzungen mit einer Beschreibung des Verstosses, des Zeitraums, der Folgen des Verstosses, des Namens des Berichterstatters und an wen der Verstoss gemeldet wurde, und des Verfahrens zur Wiederherstellung der Daten.

[1] Bemerkung: Die Protokollierung der Abfrage von ISAB-Cards mittels der ISAB Kontroll-Applikation ist technisch in der Version 1.0 nicht realisiert.

Anforderung: Sicherstellen, dass Personendaten, die von Unterauftragsbearbeiter (gemäss Art 1e) bearbeitet werden, nur in Übereinstimmung mit den Anweisungen der PK bearbeitet werden können:

ISAB stellt die Kontrolle der Unterauftragsbearbeiter durch geeignete Massnahmen sicher, unter anderem durch den Abschluss von schriftlichen Verträgen mit Unterauftragsbearbeiter, die den geltenden Datenschutzbestimmungen entsprechen, und der Überprüfung der Einhaltung dieser Vereinbarungen durch die Unterauftragsbearbeiter.

Anforderung: Sicherstellen, dass Personendaten vor versehentlicher Zerstörung oder Verlust geschützt sind:

ISAB stellt die Verfügbarkeitskontrolle durch geeignete Massnahmen sicher. Insbesondere hat ISAB ein Backup- und Wiederherstellungskonzept erstellt und umgesetzt. Backups werden regelmässig (mindestens einmal pro Tag) erstellt und ISAB ist in der Lage, Daten aus solchen Backups wiederherzustellen. ISAB wendet geeignete Verfahren an, um sicherzustellen, dass Personendaten sicher gelöscht werden, wenn sie nicht mehr verwendet werden, und dass Personendaten auf Datenträgern, die nicht mehr verwendet werden, nicht mehr abgerufen oder wiederhergestellt werden können[2]. ISAB stellt sicher, dass alle sicherheitsrelevanten Funktionen der Bearbeitungssysteme überwacht und verfügbar sind und führt geeignete Massnahmen ein, um sicherzustellen, dass jede relevante Störung unverzüglich erkannt wird.

Voraussetzung: Gewährleistung, dass Daten, die für verschiedene Zwecke erhoben wurden, getrennt verarbeitet werden können:

ISAB stellt die Trennungsregel durch geeignete Massnahmen sicher. Insbesondere können solche Datensätze durch die Auswahlfunktionen des verwendeten Systems identifiziert und getrennt werden.

Anforderung: Gewährleistung, dass die Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung von Personendaten regelmässig geprüft, beurteilt und bewertet wird:

ISAB verpflichtet sich, die Wirksamkeit der technischen und organisatorischen Massnahmen regelmässig zu prüfen, zu beurteilen und zu bewerten, die Ergebnisse dieser Prüfungen, Beurteilungen und Bewertungen zu dokumentieren und die bei diesen Prüfungen, Beurteilungen und Bewertungen festgestellten Mängel unverzüglich angemessen zu beheben.

Anforderung: Sicherstellung angemessener organisatorischer Massnahmen zum Schutz von Personendaten

ISAB sorgt für die Umsetzung angemessener organisatorischer Massnahmen zum Schutz von Personendaten. ISAB wählt, instruiert und überwacht Mitarbeiter und andere Personen, die an der Bearbeitung von Personendaten beteiligt sind, sorgfältig und angemessen. ISAB hat angemessene Geheimhaltungs- und Datenschutzrichtlinien implementiert und überprüft die Einhaltung dieser Richtlinien und Anweisungen und setzt sie durch. Mitarbeiter und andere Personen, die an der Bearbeitung von Personendaten beteiligt sind, werden regelmässig in Datenschutz und dem Schutz der Privatsphäre geschult. Organisatorische Massnahmen werden vom Anbieter ausreichend dokumentiert.

[2] Bemerkung: Die Forderung, auch Personendaten, welche sich ggf. noch auf Backup-Datenträgern befinden, zu löschen, ist nicht realisierbar.