Datenschutz-Konzept

gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018

Von

Procomm e.U.

PR-Beratung und Marketing

Geschäftsführer: Gabriela Mair

Urbangasse 21/1/11

A-1170 Wien

Email: g.mair@procomm.biz

Tel.: 0676/9083571

Erstellt am 11.05.2018

Inhalt

1. Allgemeines

1.1. Ziele und Gültigkeitsbereich

Das Ziel des Datenschutzes und der daraus resultierenden Strategie ist Unternehmensdaten soweit zu schützen, dass kein unternehmenskritischer Datenverlust eintreten kann und personenbezogene Daten nach DSGVO bestmöglich geschützt sind.
Personen und deren Daten werden nach Art.5 Z.1 auf rechtmäßige Weise, nach Treu und Glauben für festgelegte, eindeutige und legitime Zwecke verarbeitet. Sämtliche Daten werden vertraulich bestmöglich geschützt und bei Nichtverwendung bzw. durch festgelegte Fristen wieder gelöscht. Die Rechtmäßigkeit der Verarbeitung ist gegeben und wird nachfolgend nachgewiesen und wenn notwendig, durch eine Einwilligung des Betroffenen gerechtfertigt. Sämtliche Rechte der Betroffenen werden berücksichtigt und die Transparenz durch bestmögliche Information gewährleistet. Um das Datenschutzniveau hoch zu halten wird auf externe Beratungstätigkeit zurückgegriffen und Mitarbeiter laufend geschult.

1.2. Sachliche und räumliche Tätigkeit DSGVO

Wir verarbeiten als Unternehmen personenbezogene Daten von natürlichen Personen ganz oder teilweise automatisiert und haben eine Niederlassung in der EU. Wir haben zwar weniger als 250 Mitarbeiter, haben uns aber trotzdem entschlossen ein Verarbeitungsverzeichnis zu erstellen, da regelmäßig personenbezogene Daten verarbeitet werden. Als KMU/Verein haben wir unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Recht und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen ergriffen um optimalen Datenschutz zu gewährleisten.

1.3. Datenschutzbeauftragter (DSB)

Es wurde kein Datenschutzbeauftrater nach DSGVO bestellt, weil kein Kriterium erfüllt ist (Art. 37):

- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

1.4. Datenschutzberatung und -ausbildung

Dieses Datenschutzkonzept bzw. die notwendige DSGVO-Dokumentation wurde von einem geschulten und zertifizierten Berater nach besten Wissen und Gewissen mit Hilfe der Informationen des Veranwortlichen erstellt. Die Rechtsgrundlagen und weitere rechtliche Einschätzung beruhen auf den getroffenen Analysen und dem derzeitigen Rechtsverständnis.

Haftungsansprüche, welche sich auf Schäden materieller oder ideeller Art, einschließlich entgangenen Gewinn oder sonstige direkte oder indirekte Folgeschäden beziehen, sind gegenüber dem Berater ausgeschlossen. Um eine rechtlich verbindliche Absicherung zu erhalten, ist eine zusätzlich Konsultierung eines Rechtsanwalts notwendig, der die gewerbliche Sicherstellung geben kann.

2. Verfahrensverzeichnis

Referenzen: Art 30, Art 31 DSGVO, Erwägungsgründe 13, 75, 76, 82, 89

2.1. Verantwortliche

Name und Anschrift des Verantwortlichen
Procomm e.U.
Gabriela Mair
Urbangasse 21/1/11
A-1170, Wien
E-Mail: g.mair@procomm.biz
Tel.: 0676/9083571

2.2. PR Arbeit

2.2.1. Verantwortliche Person

Gabriela Mair
Urbangasse 21/1/11
1170 Wien
E-Mail: g.mair@procomm.biz
Tel.: 0676/9083571

2.2.2. Beschreibung / Zweck

Aussendungen für PR Arbeit insbesondere Fachartikel, Einladung zur Presskonferenzen, Interviews und Firmenpräsentationen

2.2.3. Kategorien der betroffenen Personen

1. PR-Adressen
Journalisten, Blogger, Influencer

2.2.4. Rechtsgrundlagen

berechtigtes Interesse (DSGVO Art. 6 Abs. 1 f)
und Erwägungsgrund 47 im Sinne des Unternehmenszwecks und des Gewerbes für Direktmarketing. Alle verwendeten Adressen sind Ansprechpersonen von Presse oder Agenturen bzw. Personen, die in öffentlichen Registern oder Verzeichnisse geführt werden. Daher wird das berechtigte und wirtschaftliche Interesse für Direktwerbung wichtiger als die möglichen Folgen der Betroffenen angesehen, da diese mit Zusendung von PR-Informationen rechnen dürfen. Informationspflicht wird eingehalten und die Möglichkeit der Abmeldung berücksichtigt.

2.2.5. Verträge , Zustimmungserklärungen oder sonstige Unterlagen

2.2.6. Kategorien der verarbeiteten Daten

Personen-/Datenkategorie	Empfänger	Löschfrist	sensible Daten
1./Persönliche Identifikationsdaten	IT-Technik	bei Inaktivität maximal 3 Jahre oder Abmeldung	-
1./Kontaktdaten	IT-Technik	bei Inaktivität max. 3 Jahre oder Abmeldung	-

2.2.7. Spezielle technische und organisatorische Maßnahmen für dieses Verfahren

2.2.8. Übermittlung an Drittstaaten

Übermittlung an USA/Fa. Cision
Garantien: Cision Vertrag, der EU-Standardklauseln enthält

2.3. Buchhaltung

2.3.1. Verantwortliche Person

Gabriela Mair
Urbangasse 21/1/11
1170 Wien
E-Mail: g.mair@procomm.biz
Tel.: 0676/9083571

2.3.2. Beschreibung / Zweck

Rechnungserstellung und Buchhaltung

2.3.3. Kategorien der betroffenen Personen

1. Kunden
ehemalige und bestehende Kunden mit Aufträgen

2.3.4. Rechtsgrundlagen

rechtliche Verpflichtung (DSGVO Art. 6 Abs. 1 c)

2.3.5. Verträge, Zustimmungserklärungen oder sonstige Unterlagen

2.3.6. Kategorien der verarbeiteten Daten

Personen-/Datenkategorie	Empfänger	Löschfrist	sensible Daten
1./Persönliche Identifikationsdaten	Banken,IT-Technik,Steuerberater	Steuerrecht nach § 132 Abs 1 BAO: 7 Jahre	-

2.3.7. Spezielle technische und organisatorische Maßnahmen für dieses Verfahren

2.3.8. Übermittlung an Drittstaaten

keine Übermittlung an Drittstaaten

2.4.E-Mail inkl. Adressverwaltung

2.4.1. Verantwortliche Person

Gabriela Mair
Urbangasse 21/1/11
1170 Wien
E-Mail: g.mair@procomm.biz
Tel.: 0676/9083571

2.4.2. Beschreibung / Zweck

E-Mail System inkl. Adressverwaltung für Kunden etc.

2.4.3. Kategorien der betroffenen Personen

1. Kunden
ehemalige und bestehende Kunden mit Aufträgen

2. Partner
Partnerfirmen

3. Interessenten

2.4.4. Rechtsgrundlagen

Erfüllung eines Vertrages (DSGVO Art. 6 Abs. 1 b)

2.4.5. Verträge, Zustimmungserklärungen oder sonstige Unterlagen

2.4.6. Kategorien der verarbeiteten Daten

Personen-/Datenkategorie	Empfänger	Löschfrist	sensible Daten
1./Persönliche Identifikationsdaten	IT-Technik	Steuerrecht nach § 132 Abs 1 BAO: 7 Jahre	-
1./Kontaktdaten	IT-Technik	Steuerrecht nach § 132 Abs 1 BAO: 7 Jahre	-
2./Persönliche Identifikationsdaten	IT-Technik	Steuerrecht nach § 132 Abs 1 BAO: 7 Jahre	-
2./Kontaktdaten	IT-Technik	Steuerrecht nach § 132 Abs 1 BAO: 7 Jahre	-
3./Persönliche Identifikationsdaten	IT-Technik	Steuerrecht nach § 132 Abs 1 BAO: 7 Jahre	-
3./Kontaktdaten	IT-Technik	Steuerrecht nach § 132 Abs 1 BAO: 7 Jahre	-

2.4.7. Spezielle technische und organisatorische Maßnahmen für dieses Verfahren

2.4.8. Übermittlung an Drittstaaten

Übermittlung an Google-Mail / USA
Garantien: Unterliegt Privacy Shield

2.5.Website

2.5.1. Verantwortliche Person

Gabriela Mair
Urbangasse 21/1/11
1170 Wien
E-Mail: g.mair@procomm.biz
Tel.: 0676/9083571

2.5.2. Beschreibung / Zweck

Zur Unternehmensdarstellung und Kontaktaufnahme inkl. Kontaktformular und weiterführenden Links

2.5.3. Kategorien der betroffenen Personen

1. Interessenten

2. Webuser
Nicht bekannte Nutzer der Website

2.5.4. Rechtsgrundlagen

berechtigtes Interesse (DSGVO Art. 6 Abs. 1 f)
bzw. vorvertragliche Maßnahmen bei Zusendung der Daten mittels Kontaktformular

2.5.5. Verträge, Zustimmungserklärungen oder sonstige Unterlagen

2.5.6. Kategorien der verarbeiteten Daten

Personen-/Datenkategorie	Empfänger	Löschfrist	sensible Daten
1./Persönliche Identifikationsdaten	IT-Technik	maximal 3 Jahre	-
1./Log-Informationen	IT-Technik	3 Monate	-
2./Log-Informationen	IT-Technik	3 Monate	-

2.5.7. Spezielle technische und organisatorische Maßnahmen für dieses Verfahren

2.5.8. Übermittlung an Drittstaaten

Übermittlung an Google Analytics / USA
Garantien: Unterliegt Privacy Shield

2.6.Social Media

2.6.1. Verantwortliche Person

Gabriela Mair
Urbangasse 21/1/11
1170 Wien
E-Mail: g.mair@procomm.biz
Tel.: 0676/9083571

2.6.2. Beschreibung / Zweck

Social Media-Betreuung im Auftrag des Kunden auf Facebook und anderen Kanälen

2.6.3. Kategorien der betroffenen Personen

1. Social-Media Nutzer

2.6.4. Rechtsgrundlagen

Erfüllung eines Vertrages (DSGVO Art. 6 Abs. 1 b)
im Auftrag des Kunden bzw. Einwillligung der Betroffenen auf den Plattformen

2.6.5. Verträge, Zustimmungserklärungen oder sonstige Unterlagen

2.6.6. Kategorien der verarbeiteten Daten

Personen-/Datenkategorie	Empfänger	Löschfrist	sensible Daten
1./Persönliche Identifikationsdaten	IT-Technik	keinen Einfluss	-

2.6.7. Spezielle technische und organisatorische Maßnahmen für dieses Verfahren

2.6.8. Übermittlung an Drittstaaten

keine Übermittlung an Drittstaaten

2.7.Newsletter

2.7.1. Verantwortliche Person

Gabriela Mair
Urbangasse 21/1/11
1170 Wien
E-Mail: g.mair@procomm.biz
Tel.: 0676/9083571

2.7.2. Beschreibung / Zweck

Für Kunden werden Newsletter erzeugt und an zur Verfügung gestellte Adressen versandt. Der Versand wird analysiert und gesteuert und eine Erfolgsstatistik bereitgestellt.

2.7.3. Kategorien der betroffenen Personen

1. Newsletter-Empfänger

2.7.4. Rechtsgrundlagen

Erfüllung eines Vertrages (DSGVO Art. 6 Abs. 1 b)
des Kunden bzw. Einwilligung der Betroffenen beim Kunden

2.7.5. Verträge, Zustimmungserklärungen oder sonstige Unterlagen

2.7.6. Kategorien der verarbeiteten Daten

Personen-/Datenkategorie	Empfänger	Löschfrist	sensible Daten
1./Persönliche Identifikationsdaten	IT-Technik	bis zum Ende des Vertragsverhältnisses mit Kunden oder bei Abmeldung	-
1./Kontaktdaten	IT-Technik	bis zum Ende des Vertragsverhältnisses mit Kunden oder bei Abmeldung	-

2.7.7. Spezielle technische und organisatorische Maßnahmen für dieses Verfahren

2.7.8. Übermittlung an Drittstaaten

Übermittlung an USA/Mailchimp Inc.
Garantien: Privacy Shield

3. Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

3.1. Vertraulichkeit

Vertraulichkeit bedeutet, dass Daten nur befugten Personen zugänglich zu machen sind. Bedroht sind nicht nur die Daten selbst sondern auch z.B. Systeme, Konfigurationen. Ein Angriff auf die Vertraulichkeit stellt die unbefugte Informationsgewinnung dar (z.B. durch das Ausspähen der login-Daten durch einen Unbefugten). Bei der Vertraulichkeit müssen Sicherheitsmaßnahmen erhoben werden, damit ein unbefugter Zugriff auf gespeicherte als auch auf übermittelte Daten verhindert werden kann.

3.1.1. Zutrittskontrolle

Zutritt fremder Personen nur mittels Gegensprechanlage, Sicherheitsschlösser und Verwaltung der Schlüsselausgabe. Bei Vermietung (falls) einzelner Büroräume werden diese einzeln versperrt

3.1.2. Zugangskontrolle

Alle Systeme sind mit Passwörter geschützt, externe Datenträger werden nicht für den Datentransfer personenbezogener Daten verwendet, Firewall sowie Antivirus-Software sind aktuell, Orbi-Router schützt Netzwerk, am Smartphone nur Daten per G-Mail, Whatsapp nur privat

3.1.3. Zugriffskontrolle

Zugriff nur durch Verantwortlichen, Passwortrichtlinien müssen eingehalten werden, Aktenvernichter werden für Listen mit personenbezogenen Daten verwendet, falls Listen ausgedruckt werden sollten

3.2.Integrität

Integrität bedeutet, dass Daten / Systeme korrekt, unverändert bzw. verlässlich sind. Ein Angriff auf die Integrität wäre z.B. die Verfälschung der Daten, wenn der Empfänger eine andere Nachricht erhält, als vom Sender abgeschickt. Die Integrität ist aber auch dann tangiert, wenn Soft- oder Hardware fehlerhaft arbeitet und falsche Ergebnisse liefert (und damit unverlässlich ist).

3.2.1. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung per Webbrowser, E-Mail-Übertragung nur mit einzelnen Mails, keine massenhafte Übertragung von Personendaten

3.2.2. Eingabekontrolle

Personenbezogene Daten in das Datenverarbeitungssystem werden ausschließlich von Berechtigten eingegeben, verändert oder entfernt, Änderungen und Löschungen von Newsletter-Empfang bzw. Abmeldung werden protokolliert und historisiert

3.3. Verfügbarkeit und Belastbarkeit

Verfügbarkeit bedeutet, dass Daten und IT-Systeme zur Verfügung stehen und von autorisierten Personen genutzt werden können, wenn dies benötigt wird. Eine unbefugte Unterbrechung z.B. durch Serverausfall oder Ausfall von Kommunikationsmitteln stellt einen Angriff auf die Verfügbarkeit dar.

3.3.1. Verfügbarkeitskontrolle

Datensicherung extern im Büro versperrt und auf Cloud-Speicher abgelegt

3.3.2. Belastbarkeit/Resilienz

Die Auslegung der Systeme ist mit genügend Spielraum versehen, DoS Angriff oder Internet-Ausfall ist keine große Bedrohung

3.4. Pseudo-, Anonymisierung und Verschlüsselung:

Resilienz ist die Fähigkeit eines Systems, trotz massiver externer oder interner Störungen wieder in den Ausgangszustand zurückzukehren. Ein technisches System wird als resilient bezeichnet, wenn das System seine Leistung trotz einer internen oder externen Störung erbringt und den Systembetrieb aufrechterhält.

3.4.1. Pseudonymisierung

für Newsletter-Adressen nicht sinnvoll

3.4.2. Verschlüsselung

externe Datenträger werden verschlüsselt, wenn für Datenübertragung personenbezogener Daten genutzt, keine massenhafte Übertragung geplant

3.5.Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Risikoanalyse, Datenschutzfreundliche Voreinstellungen, Ein Kontroll- und Verbesserungsprozess, Weiterbildung, Schulung, Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers

3.5.1. Evaluierung

laufender Kontroll und Verbesserungsprozess inkl. Weiterbildung ist etabliert, jährlicher Audit aller Maßnahmen

4. Betroffenenrechte wahren

Grundsätzlich stellen wir jedem Nutzer bzw. Betroffenen die jeweils aktuelle Version dieses Datenschutzkonzeptes auf der Homepage unter Datenschutz zur Verfügung.

Gemäß der DSGVO hat jeder Betroffene folgende Rechte:

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung (Art 17 DSGVO)
- Recht auf Einschränkung (Art 18 DSGVO)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
- Recht auf Widerspruch (Art 21 DSGVO)
- Recht auf Beschwerde bei der Datenschutzbehörde

4.1.Prozesse betreffs Betroffenenrechte

4.1.1. Allgemeines

Betroffenenrechte werden per E-Mail, Telefonisch oder persönlich vorgebracht. Kann der Betroffene seine Identität nicht zweifelsfrei angeben wird eine Führerscheinkopie verlangt. Das Verlangen des Betroffenen wird nach Identifizierung in einer Liste gespeichert und bearbeitet. Redakteur mit definitiver E-Mail-Adresse und Telefonnummer kann nach Rückfrage als identifiziert gelten.

4.1.2. Recht auf Auskunft (Art 15 DSGVO)

Der Betroffene bekommt als Pdf
- aktuelles Datenschutzkonzept
- Stammdatenblatt mit alle pb Daten
- sonstige Daten
- E-Mails

4.1.3. Recht auf Berichtigung (Art 16 DSGVO)

zu berechtigende Daten werden vom Betroffenen eingeholt und die bestehenden Daten korrigiert.
Der Betroffene bekommt als Pdf
- aktuelles Datenschutzkonzept
- Stammdatenblatt mit berichtigten pb Daten

4.1.4. Recht auf Löschung (Art 17 DSGO)

Der Betroffene bekommt per PDF

- wenn Löschung berichtigt und möglich:
  sein Stammdatenblatt ohne pb Daten (ausgenommen Name) als Nachweis, dass die Löschung erfolgt ist

- wenn die Löschung nicht möglich ist:
Bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werden wir Art 6 Z 1 lit f (berechtigte Interessen des Verantwortlichen) DSGVO geltend machen und kann daher aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall erst nach 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen die pb Daten löschen. In diesen Fällen tritt an Stelle einer Löschung der Daten eine Sperrung (Einschränkung). Nicht für die Einhaltung der Verträge notwendige Daten werden je nach Löschfristen gelöscht.

4.1.5. Recht auf Einschränkung (Art 18 DSGVO)

Der Betroffene bekommt als Pdf mit
- dem aktuellen Datenschutzkonzept

- eine Bestätigung, dass seine Daten nicht mehr verwendet werden, mit der Ausnahme für buchhalterische oder gesetzliche Zwecke

4.1.6. Recht auf Übertragbarkeit (Art 20 DSGVO)

Der Betroffene bekommt als Pdf
- aktuelles Datenschutzkonzept
- sein Stammdatenblatt mit alle pb Daten
- gemäß Art 20 Z2 DSGVO übermittle ich sein Stammdatenblatt mit alle pb Daten als Cc. an einen anderen Verantwortlichen, den der Betroffene mir genannt hat als CSV-Datei

4.1.7. Recht auf Widerspruch (Art 21 DSGVO)

Bei Verarbeitungen, die auf einer Einwilligung beruhen, ist ein Widerspruch möglich.
Im Falle einer Widerspruchsmeldung wird die Verarbeitung, falls nicht durch eine andere Rechtsgrundlage gedeckt, eingestellt und ein PDF mit der Bestätigung zugesendet.

4.2. Einwilligung sicherstellen

Die Rechtmäßigkeit der Verarbeitung pb Daten kann, sofern diese nicht der Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung dient, insbesondere durch die Einwilligung einer natürlichen Person sichergestellt werden. Dabei sind die Vorgaben der DSGVO im Detail zu beachten.
Zielsetzung

- Die Einwilligung soll durch eine freiwillige, eindeutige Handlung erfolgen, mit der bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden pb Daten einverstanden ist
- Der Verantwortliche muss nachweisen können, dass die betroffene Person ihre Einwilligung zu der Verarbeitungstätigkeit gegeben hat
- Der betroffenen Person muss zur Kenntnis gebracht werden, wer der Verantwortliche ist, für welche Zwecke ihre pb Daten verarbeitet werden und dass die Einwilligung auch verweigert oder zurückgezogen werden kann

Für welche Verfahren eine Einwilligung eingeholt wird, entnehmen Sie bitte dem Verzeichnis der Verarbeitungstätigkeiten.

5. Meldung von Datenschutzverletzungen

Die DSGVO definiert in Art 33 eine „Verletzung des Schutzes personenbezogener Daten“ (data breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Im Falle einer Verletzung des Schutzes personenbezogener Daten wird umgehend eine Konferenz mit der IT-Technik einberufen um die Schwere der Verletzung zu definieren. Im Anlassfall wird dann unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde gemeldet. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Bei einem Risiko für Betroffene werden diese ebenfalls informiert. Die Data-Breach-Konferenz wird - wenn notwendig - so schnell wie möglich vor Ort weitergeführt und alle Maßnahmen getroffen um den Schaden zu minimieren bzw. in Zukunft zu verhindern. Der Vorfall wird ausführlich dokumentiert.

6. Risikoanalyse

Referenzen: Art 24 + 25 DSGVO, Erwägungsgründe: 74-78, 81

Es wurde eine Risikoanalyse für die Tätigkeiten im Verarbeitungsverzeichnis durchgeführt. Die Tätigkeiten wurden mit Verzeichnisse der Datenschutzbehörde abgeglichen und bei weiteren Analysen konnte kein hohes Risiko für Betroffene festgestellt werden. Damit wurde auch keine Datenschutz-Folgenabschätzung durchgeführt.

7. Einwilligung sicherstellen

Die Rechtmäßigkeit der Verarbeitung pb Daten kann, sofern diese nicht der Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung dient, insbesondere durch die Einwilligung einer natürlichen Person sichergestellt werden. Dabei sind die Vorgaben der DSGVO im Detail zu beachten.
Zielsetzung
- Die Einwilligung soll durch eine freiwillige, eindeutige Handlung erfolgen, mit der bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden pb Daten einverstanden ist
- Der Verantwortliche muss nachweisen können, dass die betroffene Person ihre Einwilligung zu der Verarbeitungstätigkeit gegeben hat
- Der betroffenen Person muss zur Kenntnis gebracht werden, wer der Verantwortliche ist, für welche Zwecke ihre pb Daten verarbeitet werden und dass die Einwilligung auch verweigert oder zurückgezogen werden kann

8. Informationspflichten einführen (Art. 12 bis 14 DSGVO)

Um die Informationspflichten zu erfüllen wurden folgende Maßnahmen getroffen:
- Bereitstellung von Informationen im Internet mittels überarbeiteter Datenschutzerklärung

9. Auftragsverarbeiter-Rahmenbedingungen

Alle Vereinbarungen mit Auftragsverarbeiter wurden überprüft und ggf. angepasst. Es wurde sichergestellt, dass die Auftragsverarbeiter die Vorschriften lt. DSGVO einhalten.

10. Mitarbeiter schulen

Um Bedrohungen frühzeitig zu erkennen und Datenschutz-Verletzungen zuvor zu kommen werden Mitarbeiter initial geschult, um alle Maßnahmen der DSGVO zu kennen und danach zu handeln. Es wurde eine DSGVO- und IT-Sicherheits-Beratung in Anspruch genommen. Weiters werden laufend Weiterbildungen und Schulungen besucht.