



Datenverarbeitungsverzeichnis nach Art 30 Abs 2 EU-Datenschutz-Grundverordnung (DSGVO Auftragsverarbeiter):	Ort: Büro Kremsmünster
	Datum: 13.04.2018
	Autor: Erich Sturmair

Inhalt	
1.	Stammblatt Auftragsverarbeiter 2
1.1.	Kontaktdaten Auftragsverarbeiter: 2
1.2.	Kontaktdaten Datenschutzkoordinators: 2
1.2.1.	Systemadministrator: 2
2.	Stammblatt zum Verantwortlichen, in dessen Namen Daten verarbeitet werden, und Angaben zur Auftragsdatenverarbeitung Zwecke und Beschreibung der Datenverarbeitung: 2
2.1.	Name und Kontaktdaten des für die Verarbeitung Verantwortlichen (=Auftraggeber) 2
2.1.1.	Business Engeneering DI Christian Wolbring 2
2.1.2.	Unternehmensberatung Erich Sturmair mensch>>wissen>>ordnung 2
2.1.3.	BürgerEnergie Traunviertler Alpenvorland e.Gen. 3
2.2.	Alle Mitglieder und Kooperationspartner entsprechend der aktuellen Mitgliederliste 3
3.	Kategorien von Verarbeitungen, die im Auftrag des konkreten Verantwortlichen durchgeführt werden 3
3.1.	Cloud Computing: 3
4.	Übermittlung von personenbezogenen Daten in Drittländer, inkl. internationale Organisationen..... 4
5.	Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen..... 4
5.1.	Allgemeiner technischer Aufbau 4
5.2.	Vertraulichkeit:..... 4
5.3.	Integrität:..... 5
5.4.	Verfügbarkeit und Belastbarkeit: 5
5.4.1.	Schutz und Sicherung..... 5
5.4.2.	Verschlüsselung 6
5.4.3.	Evaluierungsmaßnahmen:..... 6



Abschnitt A:

1. Stammblatt Auftragsverarbeiter

1.1. Kontaktdaten Auftragsverarbeiter:

Expertforce e.Gen.

Geschäftsführer: DI Stephan Imbery
Rathausplatz 1, 4550 Kremsmünster
Telefon: +43 (0)720 595595
Fax: +43 (0)720 595595 99
E-Mail: office@expertforce.at
Firmenbuch: 343998f, LG Steyr

1.2. Kontaktdaten Datenschutzkoordinators:

Erich Sturmair
Adresse: wie oben
Telefon: +43 (0)699 11763897
E-Mail: erich.sturmair@expertforce.at

1.2.1. Systemadministrator:

Erich Sturmair

Abschnitt B:

2. Stammblatt zum Verantwortlichen, in dessen Namen Daten verarbeitet werden, und Angaben zur Auftragsdatenverarbeitung Zwecke und Beschreibung der Datenverarbeitung:

2.1. Name und Kontaktdaten des für die Verarbeitung Verantwortlichen (=Auftraggeber)

2.1.1. Business Engineering DI Christian Wolbring

DI Christian Wolbring
Sitz: Ziegelholz 2, 4550 Kremsmünster
Büro: Rathausplatz 1, 4550 Kremsmünster
E-Mail: office@wolbring.at
Telefon: +43 (676) 88680511

2.1.2. Unternehmensberatung Erich Sturmair mensch > > wissen > > ordnung



Erich Sturmair

Sitz: Leitensstraße 5/1, 4540 Bad Hall

Büro: Rathausplatz 1, 4550 Kremsmünster

E-Mail: office@sturmair.org

Telefon: +43 (699) 17763897

2.1.3. BürgerEnergie Traunviertler Alpenvorland e.Gen.

Geschäftsführer DI Christian Wolbring, Christian Schilcher MBA

Sitz: Pfarrhofstraße 1, 4070 4596 Steinbach an der Steyr

E-Mail: energie@leader-alpenvorland.at

Telefon: +43 (0)676 88680511

2.2. Alle Mitglieder und Kooperationspartner entsprechend der aktuellen Mitgliederliste

Ansprechadresse

Zentrales Büro ExpertForce e.Gen.: Rathausplatz 1, 4550 Kremsmünster

Telefon: +43 (0)720 595595

Fax: +43 (0)720 595595 99

E-Mail: office@expertforce.at

Die Versorgung der Mitglieder und Kooperationspartner erfolgt im Sinne Datenverarbeitungsverzeichnis von ExpertForce e.Gen. und dient dem allgemeinen Unternehmenszweck (Vergleich Statut und Geschäftsordnung).

Im Sinne von Auftragsdatenverarbeitung besteht ein Vertrag mit dem einzelnen Mitglied und geht über die normalen Versorgungszwecke hinaus.

Abschnitt C:

3. Kategorien von Verarbeitungen, die im Auftrag des konkreten Verantwortlichen durchgeführt werden

3.1. Cloud Computing:

1. File Service: zum Zwecke der Datenhaltung inklusive Datensicherung
2. Applikation Services:
 - a. Domänen Verwaltung und Domäne Name Service für alle im Büro angeschlossenen Geräte
 - b. Microsoft Exchange Server
 - c. Access Datenbank für Adress- und Rechnungsverwaltung und Teilnehmerverwaltung
 - d. WEB - Service für Expertforce.at und Wolbring.at die betriebenen Homepages
 - e. Owncloud erreichbar über Internet zur Fileverteilung nach außen



- f. Mediawiki für Unternehmensdokumentation, Qualitätsmanagement und allgemeiner Wissensdokumentation
- g. CRM – System für Bürgerenergie

- 3. Security-Services: Fortigate Firewall, Anti-Virus-Services ESET Antivirus aktuelle Version, Spamfilterung mit Fortigate Spam Wall
- 4. Anschluss ans Internet via UPC Business Fiber Power 150/20

4. Übermittlung von personenbezogenen Daten in Drittländer, inkl. internationale Organisationen

Ja ☐ Nein ☒

Wenn ja, Angabe des betreffenden Drittlandes bzw. der internationalen Organisation:

Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Binding Corporate Rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt)

Abschnitt D:

5. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

5.1. Allgemeiner technischer Aufbau

Es gibt ein internes LAN mit eigenen Domänencontroller (das WLAN ist Teil des LAN). Alle Dienste die nach außen ins WAN sind verbunden mit einem DMZ - LAN, welches mit dem internen Netz nicht direkt kommuniziert und einen gesonderten Domaincontroller verwaltet wird.

Der Server kommuniziert über unterschiedliche Netzanschlüsse mit dem lokalen LAN bzw DMZ-LAN. Der Verbindung nach außen erfolgt über Regeln eingestellt auf der Firewall und werden von dieser kontrolliert.

Der Server und die Netzwerkkomponenten sind in einem eigenen kleinen Raum (abgetrennt vom übrigen Büro) untergebracht.

Die Nutzung der Infrastruktur mit eigenen Equipment ist Grundlage der genossenschaftlichen Zusammenarbeit, daher müssen alle mit autorisierten Zugang die IT Vereinbarung unterzeichnen. Es gibt keine Arbeitsstationen im Besitz von ExpertForce e.Gen.

5.2. Vertraulichkeit:



Der Schutz vor unbefugten Zutritt während der Arbeitszeit (bei besetzten Büro) erfolgt durch die augenscheinliche Kontrolle der Mitarbeiter und dem verbindlichen versperren der Zugangstür für den Fall dass niemand im Büro ist.

Alle Personen die berechtigterweise das Büro betreten dürfen sind regelkonform unterwiesen.

Der Zugang zu den einzelnen Stationen bzw. dem Terminal des Servers ist nur mit Kenntnis eines Passwortes möglich. Alle Arbeitsstationen, die in der Domäne angemeldet sind, schalten sich nach 15 Minuten in den Ruhemodus und können nur mit Passwort wieder in Betrieb genommen werden.

Der Schutz vor unbefugten Zugriff erfolgt durch persönliche Aufsicht bei Gastzugriffen. Alle Personen mit autorisierten Zugang müssten eine EDV- Erklärung unterfertigen worin sie sich verpflichten keine Daten unbefugt zu lesen, zu kopieren, zu entfernen oder zu verändern. Für die Nutzung des Fernwartungstools (TeamViewer) sind spezielle Passworte notwendig, die nur vom Administrator vergeben werden. Eine entsprechende Ergänzung in der EDV Erklärung ist dazu vorgesehen.

Der Zugang von außen via VPN Verbindung ist Systemadministrator gestattet und entsprechend gesichert

5.3. Integrität:

Weitergabekontrolle: Es ist kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich, da nur autorisierte Personen Zugriff haben und diese nur geprüfte Speichermedien verwenden dürfen. Alle Übermittlungen erfolgen über verschlüsselte Verbindungen.

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind erfolgt durch Aufzeichnung der Anmeldungen in LOG-Dateien.

Für das File Service sind mit den Auftraggebern entsprechende Berechtigung und Zugangsstrukturen festgelegt.

5.4. Verfügbarkeit und Belastbarkeit:

5.4.1. Schutz und Sicherung

Zum Schutz gegen mutwillige und zufällige Zerstörung oder Entwendung von Daten ist die Firewall FortiGate zuständig. Diese protokolliert in einer Log-Datei alle Ereignisse mit.

Alle Daten werden regelmäßig gesichert und es gibt ein schlüssiges und verbindliches Backupkonzept. Langfristige Backups werden auf Datenträgern welche in einem gesonderten Raum im Tresor aufbewahrt werden.



Alle Unterlagen, Dokumentationen, Pläne und dergleichen zur Informationstechnologie werden regelmäßig außerhalb vom Server gespeichert.

Es gibt Notfallpläne und Vereinbarungen mit der Firma VEREX, für den Fall eines totalen Hardwareausfalls.

5.4.2. Verschlüsselung

Es gibt keine Verschlüsselung beim File Service im lokalen Netz.

E-Mails werden verschlüsselt ausgeliefert bzw. im WEB-Mail zur Verfügung gestellt.

Alle WEB-Services (Cloud, Homepage, Wiki, CRM) werden verschlüsselt (via https://) zur Verfügung gestellt.

5.4.3. Evaluierungsmaßnahmen:

Alle Arbeiten, Abweichungen, Störungen usw. werden vom Systemadministrator in einem Server Logbuch aufgezeichnet.

Risikoanalyse und Datenschutzfolgeabschätzung erfolgt im Rahmen eines jährlichen Schulungsmeetings mit allen Zugangsberechtigten.