Prager Straße 287
A-1210 Wien
Tel.: +43-1-319 60 43 410
Fax: +43-1-319 60 42 499
Email: office@adra.at

Richtlinien

Datenschutz und Datensicherheit

ADRA Österreich

	Datum:	Unterschrift Vorsitzender
Beschluss Vorstand	**30. November 2020**	
Revision 1		
Revision 2		
Revision 3		
Revision 4		

Inkrafttreten: 30. November 2020

Die vorliegenden Richtlinien zu Datenschutz und Datensicherheit ist die Erweiterung der IT-Richtlinien vom 27. Oktober 2014, nachdem die Europaweiten Datenschutzbestimmungen 2018 Inkrafttreten. Die Richtlinien sind eine verbindliche Entscheidung des ADRA Österreich Vorstandes und gelten für alle Aspekte von Daten und Information mit denen ADRA Österreich arbeitet. Jeder beteiligte Mitarbeiter ist für deren Umsetzung verantwortlich.

INHALTSVERZEICHNIS

1 EINLEITUNG

1.1 Ziel und Zweck

Diese Datenschutz- und Datensicherheitsrichtlinien sind die Grundlage zur Umsetzung der Datenschutzverordnung und den sicheren Umgang mit Daten, sowie Soft- und Hardware innerhalb von ADRA Österreich.

Das Datensicherheitskonzept dient der Optimierung der Informationssicherheit innerhalb ADRA Österreich und soll dazu beitragen, bestehende und künftige Prozesse weiter im Hinblick auf eine sichere Verarbeitung der Daten zu optimieren. Diese Richtlinien sollen den sicheren und sorgfältigen Umgang mit Daten, sowie das sichere betreiben der Hardware sicherstellen, vor allem:

- Sicherer Betrieb des Netzwerks
- Zuverlässiger und effizienter Betrieb der Computer und deren Komponenten
- Datenschutz vor Missbrauch
- Sicherer Umgang mit Daten (Datenverfügbarkeit)

Die Sicherheit unserer Informationstechnik unterteilt sich in die folgenden vier Kriterien;

Verfügbarkeit: Gewährleistung des ständigen Zugriffs

Integrität: Schutz vor Veränderungen der Daten,

Vertraulichkeit: nur autorisierte Nutzer haben Zugang zu Daten

Kontrollierbarkeit: Prüfung der Maßnahmen durch Protokollierung, um die Leistungsfähigkeit von ADRA Österreich möglichst aufrecht zu erhalten.

1.2 Geltungsbereich

Diese Datenschutz- und Datensicherheitsrichtlinien gelten für die Verantwortlichen Systemadministratoren, sowie für alle Beschäftigten von ADRA Österreich. Dazu gehören alle Festangestellten, Teilzeitangestellten und freiwilligen Mitarbeiter sowie den ADRA Österreich Vorstand.

1.3 Einhaltung von Rechtsvorschriften

Bei der Nutzung von Daten und Informationen bei ADRA Österreich sind von den Mitarbeitern besonders die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit einzuhalten. Bei Unsicherheiten im Gebrauch von Daten, soll sich der Mitarbeiter an den Geschäftsführer wenden.

2 DATENSCHUTZ

2.1 Prinzipien für die Verarbeitung Personenbezogener Daten

1. Fairness und Rechtmäßigkeit

   Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und fair erhoben und verarbeitet werden.

2. Zweckbindung

   Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

3. Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- Die Identität der verantwortlichen Stelle
- Den Zweck der Datenverarbeitung
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

4. Datenvermeidung und Datensparsamkeit

   Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

5. Speicherbegrenzung bzw. Löschung

   Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozess-bezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde oder das ADRA Archiv den Datenbestand auf seine Archivwürdigkeit für historische Zwecke bewerten konnten.

Nicht mehr benötigte personenbezogene Daten werden in regelmäßigen Abständen gelöscht. Wo diese einer bestimmten Archivierungszeit unterliegen, werden sie für den regulären Zugriff gesperrt.

6. Sachliche Richtigkeit und Datenaktualität

   Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nichtzutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

7. Vertraulichkeit und Datensicherheit

   Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

2.2 *Vertraulichkeit der Verarbeitung*

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Der Vorgesetze unterrichtet seine Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

2.3 Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren. Der verantwortliche Fachbereich kann dazu den Datenschutzverantwortlichen zu Rate ziehen. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des konzernweiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

2.4 Personenbezogene Daten

Drei Kriterien für Datensicherheit:

- **Vertraulichkeit** von Daten; Schutz vor unbefugtem Zugang und Kenntnisnahme von Dateiinhalten, etc.
- **Integrität** der Software und der Daten; Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen, Manipulation von Dateien, etc.
- **Verfügbarkeit** der Systeme; Schutz vor Diebstahl, Zerstörung, Ausfallzeiten, Verlust von Datenträgern, etc.

Bezeichnung	Personen bezogene Daten	Grundwert	Schutzbedarf	Begründung
Spender-Datenbank (STA Datenverwaltung)	Ja	Vertraulichkeit	hoch	Kenntnisnahme von Spenderdaten durch unbefugte Dritte kann erheblichen Schaden bzw. Nachteile für Betroffene bedeuten.
		Integrität	hoch	Fehlerhafte Daten können Probleme bei Antwortsendungen, ausstellen von Spendenbescheinigungen Schaden anrichten
		Verfügbarkeit	hoch	Ohne Zugriff auf die Spenderdaten können Aufgaben und Pflichten zur Spenderpflege nicht erfüllt werden.
Lohnbuchhaltung	Ja	Vertraulichkeit	hoch	Personaldaten müssen besonders geschützt werden.
		Integrität	hoch	Fehlerhafte Daten können fehlerhafte Berechnungen und Auszahlungen verursachen.
		Verfügbarkeit	mittel	Kurzfristige Ausfälle sind hinnehmbar.
Finanz-buchhaltung (SAGE)	Ja	Vertraulichkeit	hoch	Daten von Maßnahmeteilnehmern können betroffen sein. Auch Betriebs- und Geschäftsgeheimnisse können betroffen sein.
		Integrität	hoch	Anforderungen der Finanzverwaltung

		Verfügbarkeit	hoch	Tagesaktuelle Buchhaltung ist betrieblich erforderlich. Daten müssen auch für Kostenträger ggf. aktuell verfügbar gemacht werden können.
E-Mail	Ja	Vertraulichkeit	Hoch	Anträge, Verträge, Personaldaten müssen geschützt sein vor unbefugten Zugängen
		Integrität	Hoch	
		Verfügbarkeit	Hoch	Anträge und Korrespondenz mit Geldgebern unterliegen in der Applikations- und Vertragsphase strengen Fristen
Internetseite	Ja	Vertraulichkeit	Hoch	Spendenformular extern über Paypal Kontaktformular auf Office Adresse
		Integrität	Mittel	Von Profis betreut und update
		Verfügbarkeit	Hoch	Vor allem nach Katastrophen für das Spendenformular
Online-Banking	Ja	Vertraulichkeit	Hoch	
		Integrität	Hoch	
		Verfügbarkeit	Hoch	
Fileserver	Ja	Vertraulichkeit	Hoch	Zeiterfassung, Personaldaten, Projektdaten, Bilder sind streng vertraulich.
		Integrität	Hoch	Müssen geschützt sein vor nicht autorisiertem Zugang
		Verfügbarkeit	Hoch	Daten unterliegen der Archivierungspflicht unterliegen und müssen für Referenz und auditzwecken jederzeit verfügbar sein.

2.5 Dateneigentum

Alle produzierten Daten und Informationen innerhalb von ADRA Österreich sind im Eigentum von ADRA Österreich. Diese sind grundsätzlich für den internen Gebrauch bestimmt. Externer Gebrauch von Daten und Informationen erfordert einer Einwilligung des Geschäftsführers und in dessen Abwesenheit eines Vorstandsmitgliedes.

2.6 Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch den Datenschutzbeauftragten überprüft und bewertet. Die Durchführung obliegt dem ADRA Österreich Vorstand und dem Wirtschaftsprüfer. Die Ergebnisse der Datenschutzkontrolle ist durch den Datenschutzverantwortlichen dem ADRA Österreich Vorstand mitzuteilen.

2.7 Datenschutzbeauftragter

Die Aufgaben umfassen:

- Unterrichtung des Vorstands und Mitarbeiter über Datenschutzpflichten
- Überprüfen des Datenschutzes und der zugehörigen Richtlinien
- Beratung anderer Mitarbeiter zu heiklen Datenschutzfragen

- Sicherstellung der Einführung und Schulung des Datenschutzes
- Umgang mit Zugriffsanforderungen
- Genehmigung ungewöhnlicher oder umstrittener Offenlegungen personenbezogener Daten
- Weiterbildung im Bereich Datenschutz

3 DATENSICHERHEIT

3.1 Betrieb der Hardware

Ein laufender Server (Host) wo mehrere Server in virtuellen Maschinen und deren Betriebssystem laufen.

Die virtuellen Maschinen holen sich die Daten von einem Cluster mit zwei gespiegelten Servern, um einen ausfallsicheren Betrieb zu gewährleisten

Eine USV garantiert (unterbrechungsfreie Stromversorgung) und im Falle eines Stromausfalls wird es ein kontrolliertes Herunterfahren der Server ermöglichen.

Back-up Server; Stündliche Sicherung der Daten (Dokumente, Bilder, Datenbank, Finanzbuchhaltung) auf dem Server. Datenrückverfolgbarkeit 1 Jahr

Zwei identische Hardware Firewall laufen im redundanten Betrieb und dienen als Abschirmung von extern. Ein Wartungsvertrag mit einer externen Firma gewährleistet die Wartung und Pflege der Firewall.

3.2 Sicherheitskopien

Die von ADRA Österreich benützte IT-Lösung ist nachvollziehbar und die Datensicherung über den Zeitraum von maximal 12 Monaten reversibel (52 wöchentliche Backups). Einmal jährlich wird das Backup als Datenkonserve kopiert und archiviert.

3.3 Datensicherung

	Zugang	Sicherung	Verantwortlich
Projektdaten und Bilder	Alle Mitarbeiter von ADRA	Stündlich, automatische Back-up	System Administrator
Spenderdatenbank (STA Verwaltung)	Geschäftsführer Leiter PR & Fundraising Finanzmanager	Stündlich, automatische Back-up	System Administrator
Buchhaltungsdaten	Finanzmanager und Stellvertreter	Stündlich, automatische Back-up	System Administrator

3.4 Zugang zu Informationen

Der Arbeitsplatz ist von den Mitarbeitern so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein. So sind Büros nach dem Verlassen des Arbeitsplatzes grundsätzlich zu verschließen. Beim Verlassen des Arbeitsplatz-PCs muss der jeweilige Mitarbeiter sich „abmelden", so dass vor der erneuten Nutzung des IT-Systems und/oder der Applikation(en) eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

Informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

Jeder Mitarbeiter von ADRA hat Zugang zu den arbeitsspezifischen Daten auf den Laufwerken:

- smb://10.0.0.43/lwp

- smb://10.0.0.3/adra$
- Client Software für Buchhaltung/STA Verwaltung haben Zugang auf SQL Server (10.0.0.80)

3.5 Passwort-Gebrauch

Soweit technisch möglich sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Der Systemadministrator wird, soweit keine betrieblichen oder technischen Gründe entgegen sprechen, jedem einzelnen berechtigten Nutzer einen Benutzernamen sowie ein Passwort zuweisen.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten. Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor-und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345).

Passwörter sollten regelmäßig gewechselt werden. Bereits genutzte Passwörter dürfen nicht noch einmal wiederverwendet werden.

3.6 Zugangsrechte

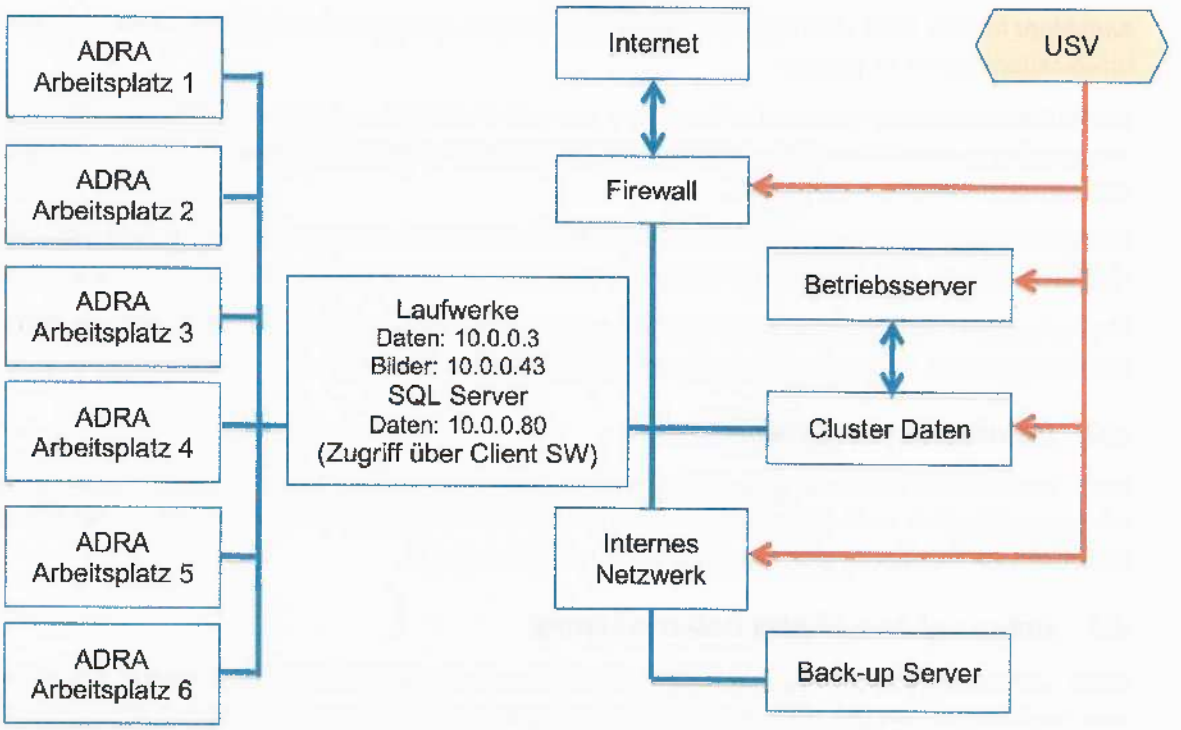
Die IT Verantwortlichen stellen sicher, dass der Zugriff auf Daten nur von autorisierten Mitarbeitern mit einem Passwort möglich ist.

	Rechtvergabe	***Zugang von ADRA Extern***	***Vergabe Rechte***
Projektdaten und Bilder	Alle Mitarbeiter von ADRA einsehbar Berechtigung zur Datenänderung nur für einen definierten Mitarbeiterkreis	System Administrator Hausdruckerei	System Administrator
Spenderdatenbank (Erfassung in SAGE, Anzeige und Auswertung in STA-Verwaltung möglich)	Datenbank-Hauptadministrator, Datenbank-Administrator	Keine	Hauptadministrator vergibt Rechte an alle Benutzer (auch an den Administrator) Administrator vergibt Rechte an andere Benutzer, jedoch nicht sich selbst
Buchhaltungsdaten	Finanzmanager und Stellvertreter	Rechnungsführer Assistent Rechnungsführer	System Administrator (nach Auftrag Rechnungsführer)

3.7 Support und Maintenance

Von den Administratoren der Kirche der Siebenten-Tags Adventisten. Im Notfall ist der System Administrator verantwortlich.

3.8 System Übersicht



4 ARBEITSPLATZ

4.1 Schutz vor schädlichen Inhalten

Zum Schutz vor Schad-Inhalten werden im Unternehmen Virenschutzprogramme eingesetzt. Insbesondere eingehende E-Mail-Kommunikation wird durch die eingesetzten Virenschutzprogramme überprüft. Dabei kann es auch zur Löschung von E-Mails und Dateianhängen kommen. Für den Fall, dass ein Mitarbeiter eine E-Mail mit einem unbekannten bzw. verdächtigen Dateianhang erhält, ist dieser verpflichtet, sich unverzüglich an den IT-Administrator zu wenden. Der unbekannte bzw. verdächtige Dateianhang darf erst nach Freigabe durch den Administrator geöffnet werden.

4.2 Schutz vor nicht verlangter Werbung („Spam")

Zum Schutz vor unverlangter Werbung durch E-Mail werden im Unternehmen so genannte Spam-Filter eingesetzt. Der Einsatz des Spam-Filters erfolgt aus betrieblichen Gründen. Durch den Spam-Filter kann es dazu kommen, dass im Einzelfall E-Mails unterdrückt oder gelöscht werden. Die Mitarbeiter sollen Sorge dafür tragen, dass zum Beispiel beim erwünschten Erhalt von E-Mail-Newsletter die entsprechenden Absender-Adressen in ihr E-Mail-Adressbuch gespeichert werden, um fehlerhafte Klassifizierungen zu vermeiden.

4.3 Schutz vor Social Engineering

Phishing: Versuch, Internetnutzern Geheimdaten zu entlocken

Spear-Phishing: Gezielter Angriff, z.B. mittels einer selektiven Liste von Ziel-E-Mail Adressen zur Erlangung von Daten durch Internetnutzer

Vishing: Per Telefonat wird versucht, den Empfänger irrezuführen und zur Herausgabe von Daten (Zugangsdaten, Passwörter, persönliche Informationen, etc.) zu bewegen.

CEO-Fraud: unter Verwendung falscher Identitäten wird versucht Empfänger, dahingehend zu manipulieren Geld zu überweisen oder Daten herauszugeben.

Smishing: Mittels SMS wird versucht Empfänger dazu zu bewegen eine Telefonnummer anzurufen und Informationenpreis zu geben.

Social Media Mining: Prozess des Erlangens von Informationen aus nutzergenerierten Inhalten auf Social-Media-Sites und mobilen Apps, um Muster zu extrahieren, Rückschlüsse auf Nutzer zu ziehen und auf diese Informationen zu reagieren.

Malware: Schadsoftware, die eine Verbindung von infizierten PCs zum Hacker im Internet aufbauen und diesem erlauben, den infizierten Rechner fernzusteuern, Daten zu manipulieren oder abzuziehen.

Ransomeware: Schadsoftware, die Dateien oder Festplatten am infizierten Rechner verschlüsselt und für die Preisgabe des Verschlüsselungspasswortes „Lösegeld" erpresst.

4.4 Installation von Software

Jeder Arbeitsplatz ist mit der grundsätzlich benötigten Software ausgerüstet. Zusätzlich benötigte Software wird ausschließlich vom System-Administrator installiert. Software von Privat oder Internet sind auf den von ADRA zur Verfügung gestellten Computern nicht erlaubt.

4.5 Daten auf dem lokalen Desktop/Laptop

Daten auf dem lokalen Computer Laufwerk werden nicht gesichert. Der Mitarbeiter hat dafür zu sorgen, dass diese Daten mittels regelmäßigen Backups gesichert sind und wo Zugriff durch andere Mitarbeiter nötig ist, diese täglich auf dem Server abgelegt werden.

4.6 Arbeiten mit Notebook

ADRA Österreich Projektleiter, die im Ausland tätig sind, arbeiten mit einem von ADRA zur Verfügung gestellten Laptop. Dieser ist mit Antivirenprogram update.

4.7 Verantwortlichkeit

Wo	Was	Job
Arbeitsplatz Computer	Ablage	• Emails laufend in Unterordner • Projekt Emails nach Ende als PDF in Projektordner • Dateien projektbezogen auf dem Server
	Löschen	• Veraltete Dateien und Dokumente wo eine neuere Version existiert • Spam und Werbe-Emails
Notebook	Datensicherung	• Monatlich und vor Abreise ins Ausland
	Löschen	• Löschen von sensiblen Daten die nicht unbedingt gebraucht werden, wenn sensible Grenzkontrollen
Homepage	Updates	• Gemeinsam mit ADRA Schweiz und ADRA Deutschland
Datenbank	Datenpflege	• Adresskorrekturen • Pflege der Kategorien/Verteiler

4.8 Software

ADRA Österreich verwendet ausschließlich lizenzierte und legale Software

5 Verarbeitungsverzeichnis

In Art. 30 DSGVO ist geregelt, dass jedes Unternehmen (von ganz wenigen Ausnahmen abgesehen) ein Verzeichnis allerseiner Verarbeitungstätigkeiten schriftlich zu führen hat. Das Verfahrensverzeichnis hat folgenden Mindestinhalt aufzuweisen:

Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen

Zwecke und Beschreibung der Datenverarbeitung:

Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

Ja / Nein

i. Wenn Ja, wann?

ii. Wenn Nein, aus welchem Grund nicht?

Detailangaben zu:

1. Kategorien der betroffenen Personen
   Lfd. Nr. *Beschreibung der Kategorien betroffener Personen (z.B. Kunden, Mitarbeiter, Lieferanten usw.)*
   a. *z.B. Kunden*
   b. *z.B. Mitarbeiter*
   c. *z.B. Lieferanten*
   d. usw.
2. Rechtsgrundlagen
3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen
4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen
   a. Kategorien der verarbeiteten Daten und ankreuzen, ob sie an Empfänger übermittelt werden

Kategorien der betroffenen Personengruppe aus (siehe Detailangaben Punkt 1)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 SDGVO, strafrechtlich relevant iSd Art 10 DSGVO	Empfänger	Empfänger	Empfänger	Empfänger	Empfänger	Empfänger
1 (oder Angabe der Personenkategorie aus Punkt 1, z.B. „Kunden“)	1								
	2								
	3								
	4								
	5								
2	6								
	7								
	8								
	9								
	10								
	11								

   b. Löschungs- und Aufbewahrungsfristen (wenn möglich)
5. Kategorien von Empfängern, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern.
   a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie z.B. UNO, OSZE)

b. Dokumentation der getroffenen geeigneten Garantien

Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit und Belastbarkeit
4. Pseudonymisierung und Verschlüsselung
5. Evaluierungsmaßnahmen

6 IT-Sicherheitskonzept

6.1 Schwachstellen und Risikoanalyse

Der Arbeitsplatz ist von den Mitarbeitern so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein.

Die Schwachstellen- & Risikoanalyse erfolgt zusammen mit der Benennung der jeweiligen Maßnahme zur Risikominimierung. Die jeweiligen Risiken werden entweder in Frageform gestellt oder auf Basis von Stichworten beantwortet (Fragenkatalog siehe Anhang A).

7 Handling von Datenschutzpannen

Trotz aller getroffener Vorkehrungen zur Einhaltung des Datenschutzes kann es zu Datenschutzpannen und einer Verletzung der Rechte der Betroffenen kommen.

Die DSGVO definiert eine Verletzung des Schutzes personenbezogener Daten als eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten führt. Dabei spielt es keine Rolle, ob diese Verletzung der Sicherheit unbeabsichtigt oder beabsichtigt war. Die DSGVO schreibt im Falle einer Datenschutzverletzung vor, alle im Zusammenhang mit der Verletzung stehenden Fakten, alle Auswirkungen der Verletzung sowie die ergriffenen Abhilfemaßnahmen zu dokumentieren.

Abhängig vom voraussichtlichen Risiko können Meldepflichten ausgelöst werden oder nicht. Ergibt die durchgeführte Risikoabschätzung, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, ist keine Meldung erforderlich. Sollte jedoch ein Risiko bestehen, ist binnen 72 Stunden, nachdem die Verletzung bekannt wurde, eine Meldung bei der Datenschutzbehörde vorzunehmen. Erfolgt die Meldung nicht innerhalb von 72 Stunden, ist die Verzögerung zu begründen.

Ergibt die durchgeführt Risikoabschätzung, dass die Datenschutzverletzung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, so sind auch unverzüglich die betroffenen Personen von der Verletzung zu benachrichtigen. Die Benachrichtigung der betroffenen Personen muss nicht erfolgen, wenn die Daten verschlüsselt waren oder durch eingeleitete Maßnahmen sichergestellt wird, dass das hohe Risiko wahrscheinlich nicht mehr besteht.

Wenn ein Mitarbeiter von ADRA eine Datenschutzverletzung feststellt, hat er diese umgehend dem ADRA Datenschutzbeauftragten und dem Geschäftsleiter mitzuteilen.

8 ANHÄNGE

8.1 Anhang A – Fragenkatalog zu Risikoanalyse

8.2 Anhang B – Gefahrenkatalog

8.3 Anhang C – Verarbeitungsverzeichnis (separate Excel Tabelle)

Reinhard Schwab
Vorsitz

Marcel Wagner
Schriftführer

Anhang A – Fragenkatalog zu Risikoanalyse (IT-System)

Frage	Antwort
Sind die vom Hersteller geforderten Installations- und Betriebsvoraussetzungen für die verwendeten Server (sicherer Stand, Stromversorgung, Temperatur, Luftfeuchtigkeit, Schutz vor Sonneneinstrahlung) geschaffen?	ja
Sind die Nutzer (einschließlich der Vertreter) von IT-Systemen aufgabenspezifisch geschult?	ja
Sind Hard- und Software inventarisiert und im Geräteverzeichnis aufgenommen?	ja
Werden bei Abwesenheit der Benutzer die Räume verschlossen?	ja
Werden die Programme einschließlich der Betriebssysteme und der systemnahen Software sowie die Datenbestände regelmäßig gesichert?	ja
Sind Ersatzgeräte bzw. Geräteteile für einen schnellen Austausch vorhanden?	Ja, bzw. in kürzester Zeit durch Händler verfügbar
Wird bei mobilen Geräten, die für dienstliche Zwecke außerhalb der Geschäftsräume eingesetzt werden, eine Dateiverschlüsselung eingesetzt?	Nein, wäre wünschenswert, verkompliziert jedoch eine Wiederherstellung der Daten
Wird Software vor deren Einsatz genehmigt bzw. freigegeben?	Ja, aber nicht technisch eingeschränkt
Kann die Benutzung des IT-Systems nur nach Eingabe einer individuellen Nutzerkennung und der Authentifizierung durch ein Passwort erfolgen?	ja
Werden die Funktionen der Benutzer von IT-Systemen und der IT-Administratoren getrennt?	ja
Sind Vertreter des IT-Administrators in ausreichender Zahl vorhanden?	ja
Werden Systemaktivitäten nachvollziehbar protokolliert?	Anlage von Daten ja, Veränderungen nein
Wird ein permanenter Virenschutz eingesetzt?	Ja nur für Windows-Rechner
Werden Datenträger nur unter Aufsicht oder in physikalisch gelöschter Form entsorgt?	CDs und DVDs werden geschredert, HDs zerstört
Sind die Zugriffsberechtigungen auf die Anwendungssoftware so weit wie möglich differenziert?	ja
Besteht eine Dokumentation der Benutzer- und Rechteverwaltung?	Ja; Server Daten STA-Verwaltung; Nein SAGE Ref. C.Gerer
Sind IT-Systeme so platziert, dass eine unbefugte Kenntnisnahme von dargestellten oder ausgedruckten Informationen (z. B. durch Besucher oder sonstige Nichtbeteiligte) ausgeschlossen wird?	ja
Werden die Tätigkeiten von Dienstleistern (Installation, Wartung, Servicetechniker) beaufsichtigt und protokolliert?	Überwacht, aber nicht protokolliert
Sind die zentralen IT-Systeme in besonders gesicherten Räumen (Sicherheitsbereich) installiert?	Zugang nur durch Admin-Büro
Sind die Zutrittsberechtigungen zum Serverraum geregelt?	ja
Werden Reinigungsarbeiten im Serverraum und technische Dienstleistungen unter Aufsicht der IT-Administratoren durchgeführt?	ja
Sind bei einer Fernwartung besondere Sicherheitsmaßnahmen vorgesehen?	ja
Werden die Daten der Fachverfahren ausschließlich auf den zentralen IT-Systemen gespeichert?	ja

Anhang B – Gefahrenkatalog

Höhere Gewalt

- Personalausfall
- Ausfall des IT-Systems
- Blitz, Feuer, Wasser
- Kabelbrand
- Unzulässige Temperatur und Luftfeucht
- Staub, Verschmutzung
- Datenverlust durch starke Magnetfelder
- Ausfall externer Netze

Menschliche Fehlhandlungen

- Nichtbeachtung von IT-Sicherheitsmaßnahmen
- Unbeabsichtigte Leitungsbeschädigung
- Gefährdung durch Reinigungs- oder Fremdpersonal
- Fehlerhafte Nutzung des IT-Systems
- Fehlerhafte Administration des IT-Systems
- Übertragung falscher oder nicht gewünschter Daten
- Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- Unbeabsichtigtes Löschen von Programmen und/oder Daten
- Unerlaubte private Nutzung des dienstlichen SystemsUnstrukturierte Datenhaltung

Technische Mängel

- Ausfall der Stromversorgung
  Ausfall interner Versorgungsnetze
  Ausfall vorhandener Sicherungseinrichtungen
- Spannungsschwankungen/Überspannung/ Unterspannung
- Defekte Datenträger
- Bekanntwerden von Softwareschwachstellen
- Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- Fehlende Authentisierungsmöglichkeit zwischen Server und Arbeitsstation
- Verlust gespeicherter Daten
- Absenden von Daten an einen falschen Empfänger durch Fehlverbindung
- Übertragungsfehler
- Informationsverlust bei unzureichender Speicherkapazität
- Datenverlust bei erschöpftem Speichermedium
- Schwachstellen oder Fehler in Standardsoftware
- Nicht getrennte Verbindungen
- Ausfall einer Datenbank
- Verlust von Daten einer Datenbank
- Verlust der Datenbankintegrität/-konsistenz
- Ausfall oder Störung von Netzkomponenten

Vorsätzliche Handlungen

- Manipulation/Zerstörung von IT-Geräten oder Zubehör
- Manipulation an Daten oder Software
  Unbefugtes Eindringen in ein Gebäude
  Diebstahl, Vandalismus, Anschlag
- Abhören von Leitungen
- Manipulation an Leitungen
- Unberechtigte IT-Nutzung
- Missbrauch von Fernwartungszugängen
- Gefährdung bei Wartungsarbeiten durch internes Personal
- Gefährdung bei Wartungsarbeiten durch externes Personal
- Systematisches Ausprobieren von Passwörtern
- Missbrauch von Benutzerrechten
- Missbrauch von Administratorrechten
- Trojanische Pferde
- Diebstahl bei mobiler Nutzung des IT-Systems
- Computer-Viren
- Unberechtigtes Kopieren der Datenträger
- Eindringen in Rechnersysteme über Modem oder externe Schnittstellen
- IP-Spoofing
- Missbrauch der Datenübertragung
- Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit
- Netzanalyse-Tools

Organisatorische Mängel

- Fehlende oder unzureichende Anweisungen bzw. Regelungen
- Unzureichende Kenntnisse der bestehenden Regelungen
  Fehlende oder ungeeignete Betriebsmittel
  Unzureichende Kontrolle der IT-Systeme
- Fehlende oder unzureichende Wartung
  Unbefugter Zutritt zu schutzbedürftigen Räumen
  Mangelhafte Anpassung an den technischen Stand
  Unzureichende Dokumentation der Verkabelung
  Unzureichend geschützte Verteiler
  Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
- Vertraulichkeitsverlust schutzbedürftiger Daten
- Ungeordneter Benutzerwechsel auf Arbeitsstationen
- Mangelhafte Kennzeichnung der Datenträger
- Unzureichendes Schlüsselmanagement bei Verschlüsselung
- Fehlende Auswertung von Protokolldaten
- Fehlendes oder unzureichendes Test- und Freigabeverfahren
- Fehlende oder unzureichende Verfahrensdokumentation
  Softwaretest mit „Echtdaten"
- Unzureichender Schutz der Bedieneroberfläche der Arbeitsstationen
- Unzureichende Leitungskapazitäten
- Nicht gesicherter Aufstellungsort von Servern

• Unberechtigte Ausführung von Netzmanagementfunktionen • Missbrauch von Netzwerkkomponenten • Unberechtigter Anschluss von IT-Systemen an ein Netz • Unberechtigter Zugang zu den Netzkomponenten • Missbräuchliche E-Mail-Nutzung • Vortäuschen eines falschen Absenders • Mitlesen von E-Mails oder sonstigen Verfahrensdaten • Ausspähen der internen gespeicherten Daten bei Internetnutzung	• Fehlende oder unzureichende Aktivierung von Sicherheitsmechanismen • Ungeeignete Einschränkung der Benutzerumgebung • Unkontrollierter Aufbau von Kommunikationsverbindungen • Konzeptionelle Schwächen des Netzes und der Serverstrukturen • Ungesicherter Datenträgertransport • Ungeeignete Entsorgung der Datenträger • Fehlende oder unzureichende Schulung der Mitarbeiter und der IT-Betreuer • Ungeordnete E-Mail-Nutzung