NewDefinition GmbH
Datenschutz-Dokumentation

Maßnahmen zur Erfüllung der Europäischen Datenschutzgrundverordnung (EU-DSGVO)
und dem neuen Bundesdatenschutzgesetz (BDSG-Neu)
im Besonderen sowie allgemeiner Datenschutzanforderungen
für alle Produkte der NewDefinition GmbH

gültig ab 25.05.2018

E N T W U R F 18.04.2018

Einleitung

Die NewDefinition GmbH ist sich der Bedeutung des Schutzes der personenbezogenen Daten und der Sicherheit dieser Daten bewusst. Sie verpflichtet sich, die diesbezüglich anwendbaren Gesetze, insbesondere die Europäische Datenschutzgrundverordnung (EU-DSGVO) und das deutsche Bundesdatenschutzgesetz (BDSG) zu beachten und ergreift erforderlichen Sicherheitsmaßnahmen zum Schutz, zur Geheimhaltung und Unversehrtheit der Daten gemäß dem aktuellen Stand der Technik und der Schutzbedürftigkeit der Daten.

Die NewDefinition GmbH bietet mit der Software die Möglichkeit einer datenschutzkonformen Datenverarbeitung und richtet sich bei den ihr als Software- und Hostinganbieter obliegenden Aufgaben und Pflichten nach der der europäischen und deutschen Datenschutzgrundverordnung. Für die Datenhaltung und -verarbeitung ist der Kunde als Erheber, Inhaber und Verwender der Daten Verantwortlicher im Sinne der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und des deutschen Bundesdatenschutzgesetzes (BDSG).

Die Datenschutz-Anforderungen ergeben sich aus den allgemeinen Grundsätzen der Europäischen Datenschutzgrundverordnung (EU-DSGVO Kapitel II Artikel 5 Absatz 1) sowie dem deutschen Bundesdatenschutzgesetzt (BDSG §47) und decken (i) Rechtmäßigkeit und Transparenz, (ii) Zweckbindung, (iii) Datenminimierung, (iv) Richtigkeit, (v) Speicherbegrenzung, (vi) Integrität und Vertraulichkeit sowie (vii) Rechenschaftspflicht durch den Verantwortlichen ab.

Den Datenschutzanforderungen wird insgesamt Rechnung getragen durch (a) Datenschutzvorkehrungen innerhalb der Software, (b) Technische und Organisatorische Maßnahmen an Bürostandoren, (c) Technische und Organisatorische Maßnahmen sowie Zertifizierungen an Serverstandorten und (d) Richtlinien und Handlungsempfehlungen für den Kunden.

Nicht personenbezogene Daten bedürfen in der Regel keines besonderen Schutzes. Sie werden daher grundsätzlich nicht verschlüsselt und können u.a. sowohl per E-Mail versendet, in Cloud-Accounts oder auf Austausch-Datenträgern temporär oder für die Dauer der Kundenbeziehung gespeichert und anderweitig ohne Datenschutzmaßnahmen verarbeitet werden. Sie sind von dieser Datenschutz-Dokumentation nicht betroffen.

Inhalte

A - Datenschutzvorkehrungen innerhalb der Software

Funktionen und Programmcode der Software bieten umfangreiche Schutzmaßnahmen für den geeigneten Umgang mit personenbezogenen Daten. Die Grundsätze der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und des deutschen Bundesdatenschutzgesetzes (BDSG) werden eingehalten und direkt ableitbare technische Maßnahmen sind im aktuellen Stand der Technik umgesetzt. Dies gilt sowohl für die generelle Funktionsweise der Software (data protection by design) als auch die vorgegebenen Grundeinstellungen (data protection by default).

Die fortlaufende Entwicklung des Stands der Technik in den Bereichen Software und Internet macht eine ständige Weiterentwicklung der Datenschutzmaßnahmen innerhalb der Software erforderlich. Diesem Umstand ist sich die NewDefinition GmbH bewusst und arbeitet fortlaufend an der Weiterentwicklung der Software insbesondere auch in Hinblick auf den Datenschutz.

Die im Folgenden beschriebenen Datenschutzvorkehrungen innerhalb der Software spiegeln den aktuellen Stand wieder und werden sich fortlaufend erweitern, anpassen und gegebenenfalls auch neu fokussieren. Einen vollständigen Schutz der Daten können diese Maßnahmen allein nicht bieten und müssen daher durch technische und organisatorische Maßnahmen an den Standorten der NewDefinition GmbH sowie des Kunden ergänzt werden.

1. Abgabe einer Einwilligung zur Verarbeitung personenbezogener Daten

Bei der Registrierung als Nutzer oder Einzelbuchungen, die keine vorherige Registrierung erforderlich machen (z.B. Anmeldung zur Teilnahme einer Veranstaltung als Gast) wird immer die Einwilligung zur Erhebung und Verarbeitung personenbezogener Daten abgefragt. Ohne eine Zustimmung ist eine Registrierung oder Buchung technisch nicht möglich. Die Texte zur Einwilligung (Datenschutzhinweise, Widerspruchsregelungen etc.) müssen vom Kunden bereitgestellt und im System gepflegt werden.

2. Nachweis der Einwilligung zur Verarbeitung personenbezogener Daten

Die vom Nutzer erteilte Einwilligung zur Datenverarbeitung wird nachweisfähig dokumentiert. Für jede erteilte Einwilligung wird protokolliert, (i) wann diese auf Basis welcher (ii) Datenschutzhinweise (iii) durch wen (Nutzerangaben mit mindestens Name und E-Mail-Adresse) über welchen (iv) Zugang (IP-Adresse) abgegeben wurden.

3. Auskunftsrecht

Jeder Nutzer hat ein Auskunftsrecht zu den von ihm erhobenen und verarbeiteten personenbezogenen Daten. Hierzu gibt es für Administratoren eine Übersichtseite zu jedem Nutzer, welche alle vorhandenen Daten aufgelistet.

4. Recht auf Berichtigung

Jeder Nutzer kann verlangen, die zu ihm gespeicherten Daten zu korrigieren oder zu aktualisieren. Dies ist im Portal nach entsprechender Anmeldung jedem Nutzer selbstständig für die zentralen personenbezogenen Daten möglich. Diese und alle weiteren Daten kann jederzeit ein Administrator ändern z.B. auf Weisung des Nutzers.

5. Recht auf Datenbereitstellung

Jeder Nutzer kann die zu ihm gespeicherten Daten eigenständig in einem maschinenlesbaren gängigen csv-Datenformat herunterladen.

6. Recht auf Löschen/Vergessenwerden

Jeder Nutzer kann jederzeit sein Nutzerprofil löschen und eine ggf. damit verbundene Mitgliedschaft kündigen. Der Nutzer kann dabei seine Daten sofort löschen oder noch für die verbleibende Mitgliedschaftslaufzeit bestehen lassen und dann automatisch zum Ende der Mitgliedschaft löschen lassen. Einige Daten können vom Kunden (Verantwortlichen) aus buchhalterischen und/oder rechtlichen Gründen weiter genutzt werden. Alle anderen Daten werden spä-

testens nach 4 Wochen vom System sowohl im Echtbetrieb wie auch der Datensicherung gelöscht. Die Löschung erfolgt in 2 Stufen: zunächst werden alle Daten des Nutzers nicht mehr sichtbar für andere Nutzer und historische Einträge wie z.B. bei Kommentaren anonymisiert, dann erfolgt die endgültige und unwiderrufliche Löschung der personenbezogenen Daten. Damit ist auch eine Einschränkung der Verarbeitung aller oder ausgewählter personenbezogener Daten technisch möglich.

7. Datensicherheit

Alle Pflichtangaben eines Nutzerprofils, die insbesondere die besonders schutzbedürftigen Stammdaten eines Nutzers (Name, Wohnort, Kontaktdaten etc.) umfassen, die direkten Rückschluss auf die Person zulassen, werden verschlüsselt in den Datenbanken abgelegt. Freiwillige Zusatzangaben, die keinen direkten Rückschluss auf die Person zulassen und deren Angabe nicht verpflichtend ist (Angaben zur Ausbildung/Studienverlauf, Arbeitgeber und Position etc.) fallen nicht darunter.

8. Datentransferverschlüsselung

Jeglicher Datentransfer über Standardbrowser mit dem System wird standardmäßig durch ein eigenes domain-validiertes SSL-Zertifikat mit bis zu 256-Bit und Sicherheitsanzeige im Browser verschlüsselt.

9. Datensicherung

Die im System angelegten Daten werden regelmäßig automatisch gesichert. Diese Sicherungen beinhalten den Status des Systems und seiner Inhalte zum Zeitpunkt der Sicherung. Im Falle eines Ausfalls des Systems kann so eine nicht mehr als einen oder zwei Tage alte Sicherung binnen 5 Werktagen eingespielt werden und damit den gemäß der Sicherung aktuelle Stand des Systems wiederhergestellt werden.

10. Datentrennung

Jeder Kunde nutzt das System in einer vollständig eigenen Instanz ohne Überschneidungen zu anderen Kunden oder gemeinsame Datenhaltung. Daten einzelner Kunden sind logisch voneinander getrennt.

11. Zugang

Jede Anmeldung am System ist nur mit einer Kombination aus individuellem Nutzernamen/E-Mail-Adresse und Passwort möglich. Passwortvergabe erfolgt durch den Nutzer selber. Passwörter sind für keine andere Person im Klartext einsehbar. Administratoren können Passwörter manuell überschreiben. Verbindliche Passwortrichtlinien erfordern mindestens 8 Zeichen mit mindestens einem Klein-, einem Großbuchstaben sowie einer Zahl und einem Sonderzeichen. Eine jährliche Erinnerung an die Passwort-Aktualisierung kann optional eingestellt werden.

12. Automatisches Session-Timeout

Eine inaktive Anmeldung wird automatisch nach 24h abgemeldet (automatisches Session-Timeout). Hat der Nutzer bei der Anmeldung die Option „angemeldet bleiben“ aktiviert, erfolgt die automatische Abmeldung dagegen nach 180 Tagen.

13. Rechte und Rollen

Rechte und Rollen können individuell durch den Kunden-Administrator festgelegt und administriert werden. Normalerweise erhalten normale Nutzer nur sehr eingeschränkte Rechte, während Administratoren erweiterte Rechte erhalten. Nutzer dürfen jeweils nur ihr eigenes Profil anlegen, anpassen/ändern oder löschen. Administratoren dürfen dagegen alle Nutzerprofile administrieren und auch löschen. Erweiterte Benutzerrechte als Administrator werden nur durch den Kunden-Administrator vergeben. Der Kunde erhält mindestens ein Administratorenkonto und kann selbstständig weitere Administrationsrechte vergeben. Die NewDefinition GmbH erhält lediglich ein Administratorenkonto zur Systempflege.

14. Protokollierung

Wesentliche Datenänderungen und Verarbeitungsvorgänge insbesondere an den personenbezogenen Daten hinsichtlich Erhebung, Veränderung, Abfrage per Download sowie Löschung werden protokolliert. Änderungen werden mit ausführendem Nutzer, Datum und Uhrzeit sowie betroffenen Datenfeldern protokolliert. Nicht protokolliert wird die inhaltliche Änderung von welchem Wert auf welchen konkreten Wert geändert wurde.
Jeder Download von Nutzerdaten wird ebenfalls mit ausführendem Nutzer/Administrator, Datum und Uhrzeit, Datenfeldern sowie betroffenen Nutzer-IDs oder mindestens der Anzahl an Datensätzen protokolliert.
Protokolle werden am Ende des auf die Protokollierung nachfolgenden Jahres gelöscht oder anonymisiert.
Offenlegung einschließlich Übermittlung per Schnittstellen (sofern vom Kunden beauftragt und für diesen umgesetzt) werden durch eine allgemeine Schnittstellenbeschreibung dokumentiert.
Eine automatisierte Kombination von Daten erfolgt innerhalb der Software nicht.

15. Penetrationstest

Regelmäßige Penetrationstests um Schwachstellen und konkrete „unsichere“ Codestellen zu identifizieren mindestens zwei Mal im Jahr. Danach Dokumentation und umgehende Behebung der Schwachstellen und Ausspielung mit dem nächsten Update. Im Bedarfsfall kritischer Sicherheitslücken erfolgt eine direkte Ausspielung im Rahmen eines Sicherheitsupdates.

16. Datensparsamkeit

Seit jeher gilt der Grundsatz, nur so wenige personenbezogene Daten wie unbedingt erforderlich zu erheben, zu speichern und zu verarbeiten. Dies steht teilweise im Widerspruch zu den Zielen und Zwecken von Kontaktnetzwerken und Alumni-Portalen, ist aber dennoch gesetzlich vorgegeben. Um den Datenhaushalt sinnvoll zu begrenzen, wird eine Statistik/fortlaufendes Reporting generiert, welches die prozentuale Nutzung/Ausfüllungsgrad von Profildatenfeldern über alle Nutzer eines Kunden ausweist. So kann jeder Kunde selber ersehen, welche Profildatenfelder in seinem Netzwerk nicht oder kaum genutzt werden und daher generell aus der Profilabfrage zu löschen wären.

B - Technische und Organisatorische Maßnahmen an Bürostandorten

Die nachfolgenden technischen und organisatorischen Maßnahmen werden am Bürostandort in Wiesbaden zugesichert.

1. Zutrittskontrolle
    - Alarmanlage
      Derzeit installiert ist eine Alarmanlage der Firma BOSCH mit Alarmgeber an der Eingangstür sowie Bewegungssensoren im Flur. Fenster sind im 3. OG nicht alarmgesichert. Die Alarmanlage ist per ISDN aufschaltbar und mit einer Alarmzentrale verbunden.
    - Manuelles Schließsystem und Sicherheitsschlösser mit Schlüsselregelung (Schlüsselausgabe etc.)
      IKON-Sicherheitsschließanlage mit Schlüsselkarte für sowohl den Zugang zu Treppenhaus, der Tiefgarage als auch der Büroeingangstür. Schlüssel werden nur an Geschäftsführung und ausgewählte Mitarbeiter ausgegeben.
    - Sorgfältige Auswahl von Reinigungspersonal
      Sowohl Reinigung durch Mitarbeiter selbst als auch Grundreinigung durch externes Putzpersonal über ortsansässige deutsche Unternehmen mit entsprechender vertraglicher Zusicherung von Datenschutz und Vertraulichkeit.

2. Zugangskontrolle
    - Authentifikation mit Benutzername / Passwort
      Jede Anmeldung am System ist nur mit einer Kombination aus individuellem Nutzernamen/E-Mail-Adresse und Passwort möglich.
    - Zuordnung von Benutzerrechten
      Die NewDefinition GmbH führt je Kunde ein Administratorenkonto zur Systempflege. Auf dieses Administratorenkonto haben ausschließlich die Geschäftsführung und geschulte Support-Mitarbeiter Zugriff.
    - Verschlüsselung von mobilen Datenträgern
      Einsatz von USB-Laufwerken organisatorisch ausgeschlossen.
    - Verschlüsselung von Datenträgern in Laptops / Notebooks
      Datenträger in Laptops sind stets verschlüsselt mit *FileVault* (Apple)

3. Zugriffskontrolle
    - Abgesicherter Serverzugriff
      Einsatz von VPN-Technologie. Zugriff auf die Server erfolgt stets per SFTP und einer gesicherten VPN-Verbindung.
    - Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
      Verbindliche Passwortrichtlinien erfordern mindestens 8 Zeichen mit mindestens einem Klein-, einem Großbuchstaben sowie einer Zahl und einem Sonderzeichen. Erinnerung an Aktualisierung erfolgt halbjährlich.
    - Sichere Aufbewahrung und Verschlüsselung von Datenträgern
      Keine Verwendung externer portabler Datenträger.

4. Weitergabekontrolle
    - SSL-Verschlüsselung
      Jede Kundeninstanz ist stets SSL-verschlüsselt. Eigenes domain-validiertes SSL-Zertifikat mit bis zu 256-Bit und Sicherheitsanzeige im Browser.

- E-Mail-Verschlüsselung (teilweise)
  Versand von Nutzerinformationen oder anderen vertraulichen Inhalten per E-Mail organisatorisch ausgeschlossen. E-Mail-Archivierung ausschließlich verschlüsselt.
- Kein physischer Transport von Datenträgern, da keine Nutzung mobiler Datenträger erfolgt (Laptops mit eingebauten Festplatten ausgenommen).

5. Eingabekontrolle

- Protokollierung der Eingabe, Änderung und Löschung von Daten
  Wesentliche Datenänderungen insbesondere an den Datenbanken werden protokolliert. Zugriff je Nutzer wird mit Datum und Uhrzeit protokolliert.
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
  Datenänderungen erfolgen nur über MySQL oder PHP durch direkten Entwicklereingriff und nicht über Applikationen.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
  Keine Benutzergruppen zulässig. Jede Änderung erfolgt durch ein dediziertes Nutzerkonto.
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt ausschließlich auf Basis des Berechtigungskonzeptes

6. Auftragskontrolle

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
  Bestehende Subunternehmer alle zertifiziert nach DIN ISO/IEC 27001. Keine weitere Kontrahierung von Subunternehmern oder Auftragnehmern vorgesehen. Im Bereich Entwicklung ausschließlich bei Weiterentwicklung von Funktionalitäten ohne Zugriff auf Kundendaten.
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
  Bestandteil des Anstellungsvertrages sowie einer gesonderten Datenschutzerklärung.
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
  Auf Weisung des Kunden und nach Beendigung des Vertragsverhältnisses werden alle kundenbezogenen Daten gelöscht. Kontrolle erfolgt durch die Geschäftsführung.

7. Verfügbarkeitskontrolle (reduziert am Bürostandort, erweitert am Serverstandort)

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Serverräume nicht unter sanitären Anlagen

8. Trennungsgebot

   - Logische Mandantentrennung (softwareseitig)
     Jeder Kunde wird als eigene logische Instanz aufgebaut, strikt getrennt von anderen Kundeninstanzen ohne jegliche Verknüpfung.
   - Festlegung von Datenbankrechten
     Stark eingeschränkte Zugriffsrechte auf die Datenbanken. Derzeit nur für Geschäftsführung.
   - Trennung von Produktiv- und Testsystem
     Test- und Produktinstanzen stets logisch voneinander getrennt. Das initiale Testsystem wird mit Abnahme in das Produktivsystem überführt. Spätere Testsysteme nur nach Bedarf und vor dem Ausspielen größerer Updates zwecks vorherigem Test

C - Technische und Organisatorische Maßnahmen sowie Zertifizierungen an Serverstandorten

Die NDG hat das Recht, das System auf eigenen Servern oder denen eines professionellen Hosting-Unternehmens zu hosten und zur Erbringung ausgewählter Dienste weitere Dienstleister und deren Software einzubinden. Dies erfolgt ausschließlich in einem mit dem Kunden abgestimmten Maß und unter Beachtung der Einhaltung des Datenschutzes. Eine Datenübertragung oder Verarbeitung in Drittländern außerhalb der Europäischen Union findet dabei zu keinem Zeitpunkt statt.

1. Hosting

Das System wird in der Regel auf Servern in professionell geführten Rechenzentren von renommierten Hosting-Anbietern betrieben („gehostet“). Aktuell ist der Serverstandort die *Hetzner Online GmbH*. Der Standort hat eine Zertifizierung nach DIN ISO/IEC 27001. Bei einem eventuellen, aber derzeit nicht geplanten Umzug werden mindestens vergleichbare Maßnahmen auch an eventuell neuen Standorten der NewDefinition GmbH zugesichert.

Der international anerkannte Standard für Informationssicherheit bescheinigt der Hetzner Online GmbH, dass ein geeignetes Informationssicherheitsmanagementsystem, kurz ISMS, implementiert und adaptiert wurde. Das ISMS findet an den Standorten Nürnberg und Falkenstein bei der Infrastruktur und dem Betrieb der gesamten Datacenterparks Anwendung und wurde durch die FOX Certification geprüft.
Das Zertifikat weist ein adäquates Sicherheitsmanagement, die Sicherheit der Daten, die Vertraulichkeit der Informationen und die Verfügbarkeit der IT-Systeme nach. Es bestätigt zudem, dass die Sicherheitsstandards kontinuierlich verbessert und nachhaltig kontrolliert werden.

Das Zertifikat kann hier eingesehen werden: https://www.hetzner.de/pdf/FOX_Zertifikat_de.pdf

Die Hetzner AG stellt an Serverstandorten folgende Maßnahmen sicher:

I. Vertraulichkeit
- Zutrittskontrolle
    - Datacenterparks in Nürnberg und Falkenstein
        - elektronisches Zutrittskontrollsystem mit Protokollierung
        - Hochsicherheitszaun um den gesamten Datacenterpark
        - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
        - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
        - 24/7 personelle Besetzung der Rechenzentren
        - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
        - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
    - Verwaltung
        - elektronisches Zutrittskontrollsystem mit Protokollierung
        - Videoüberwachung an den Ein- und Ausgängen
- Zugangskontrolle
    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert
- Zugriffskontrolle
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.
- Datenträgerkontrolle

- Datacenterparks in Nürnberg und Falkenstein
  - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wiedereingesetzt.
  - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).
- Trennungskontrolle
  - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- Pseudonymisierung
  - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)
- Weitergabekontrolle
  - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung. Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- Eingabekontrolle
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
- Verfügbarkeitskontrolle
  - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leitungen des Hauptauftrages.
  - Einsatz von Festplattenspiegelung.
  - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
  - Einsatz von Softwarefirewall und Portreglementierungen.
  - Dauerhaft aktiver DDoS-Schutz.
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);
  - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).
- Auftragskontrolle
  - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
  - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
  - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

2. E-Mail-Versand

Für den geeigneten Massenversand von E-Mails müssen besondere Anforderungen bedacht werden (z.B. zeitversetzter Versand, Anti-Viren-Schutz, Queue-Prozesse etc.). Daher nutzt das

System die Amazon Cloud von Amazon Web Services (AWS). Dies stellt schnellen, sicheren und professionellen Versand und Zustellung von E-Mails sowie Newslettern sicher.

Die Datensicherheit hat bei AWS höchste Priorität. In über 190 Ländern werden Services für hunderttausende Einrichtungen, einschließlich Großunternehmen, Bildungseinrichtungen und Regierungsbehörden erbracht. Kunden, darunter auch Finanzdienstleister und Dienstleister aus dem Gesundheitswesen, vertrauen AWS mitunter ihre sensibelsten Informationen an.
AWS ist so konzipiert, dass Kunden Kontrolle über ihre Inhalte haben, einschließlich wo und wie sie gespeichert werden, sowie wer Zugriff darauf hat. AWS ist nach DIN ISO/IEC 27001 zertifiziert.

Das Zertifikat kann hier eingesehen werden: https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf

Die an AWS übermittelten Daten umfassen nur die Adressierung der E-Mail (E-Mail-Adresse) sowie innerhalb der E-Mail befindlichen Daten (z.B. individuelle Anrede) und können so jederzeit vom Kunden selber gesteuert werden. Die Daten werden einzig zu dem übermittelten Zweck des Versands eine E-Mail-Kommunikation temporär verarbeitet. Eine permanente Datenspeicherung erfolgt bei AWS nicht.
Auch wenn es sich bei AWS um ein amerikanisches Unternehmen handelt, werden die Daten nicht ins außereuropäische Ausland gegeben, da die Verarbeitung am AWS-Standort in Irland erfolgt.

3. Webseitenstatistiken

Zur Erhebung, Verarbeitung und grafischen Aufbereitung anonymisierter Webseitenstatistiken (z.B. Seitenaufrufe, Verweildauer, Absprungraten etc.) nutzt das System eine für jeden Kunden eigenständige Installation der Open-Source-Komponente Matomo (www.matomo.org, ehemals Piwik). Die hierbei gespeicherten Daten sind nicht personenbezogen und vollständig pseudonymisiert.

Das Plugin auf Basis der Open-Source-Komponente Matomo kann jederzeit ausgeschaltet werden.

D - Richtlinien und Handlungsempfehlungen für den Kunden

Zur Sicherstellung des Datenschutzes ist insbesondere auch der Kunde, der im Sinn der Europäische Datenschutzgrundverordnung (EU-DSGVO) der Verantwortliche ist, zu umfangreichen Datenschutzmaßnahmen verpflichtet. Die Verpflichtungen werden im Folgenden nicht vollständig abgebildet, sondern lediglich auf zentrale Richtlinien und Handlungsempfehlungen hingewiesen, die im Zusammenspiel mit den in den vorherigen Kapiteln beschriebenen Maßnahmen mindestens erforderlich sind.

1. Nutzungsbedingungen, Datenschutzhinweise und Widerspruchsklauseln

Die EU-DSGVO fordert, die Einwilligung einer Person in die Verarbeitung ihrer personenbezogenen Daten einzuholen, bevor die Daten erhoben und verarbeitet werden. Dies muss zum Zeitpunkt der Datenerhebung geschehen und verschiedenen Anforderungen gerecht werden. Insbesondere soll die Person über die Art der Verarbeitung informiert werden. Entsprechende Nutzungsbedingungen, Datenschutzhinweise und Widerspruchsklauseln sind vom Kunden zu erstellen und bereitzustellen. Die NewDefinition GmbH ist hier gesetzlich nicht dazu berechtigt, Rechtsberatung zu geben oder Vorlagen und Muster bereitzustellen. Im Internet finden sich jedoch frei zugängliche Generatoren, um solche Dokumente zu erstellen (z.B. unter https://www.activemind.de/datenschutz/datenschutzhinweis-generator/).

2. Verbote

Die Erhebung und Verarbeitung bestimmter personenbezogener Daten ist gemäß EU-DSGVO Kapitel II Artikel 9 verboten. Es bestehen zwar Ausnahmeregelungen, aber die NDG wird Datenfelder zur Erhebung von Daten, die Rückschlüsse erlauben auf (i) rassische oder (ii) ethnische Herkunft, (iii) religiöse Einstellung, (iv) politische Meinung, (v) Weltanschauung oder (vi) Gewerkschaftszugehörigkeit nicht umsetzen. Sofern der Kunde dies im Rahmen der möglichen Individualisierung von Datenfeldern selber tut, ist er hierfür selbst verantwortlich und muss sicherstellen, dass die Einwilligung in deren Verarbeitung durch den Nutzer zudem „ausdrücklich“ erfolgt.

3. Verzeichnis über Verarbeitungstätigkeiten und Datenschutz-Folgeabschätzung

Organisationen ab 250 Mitarbeitern müssen gemäß EU-DSGVO ein Verzeichnis über die Verarbeitungstätigkeiten von personenbezogenen Daten führen. Die Einschränkung besteht im scheinbar BDSG nicht. Die NewDefinition GmbH tut dies als Auftragsverarbeiter gemäß BDSG §70 und speichert daher Namen und Kontaktdaten jedes Verantwortlichen (aller Nutzer mit Administrationsrechten) sowie des Datenschutzbeauftragten jedes Kunden. Der Datenschutzbeauftragte ist dazu künftig von jedem Kunden in der Administration in den Grunddaten anzugeben.
Der Kunde muss selber entscheiden, ob er ein Verzeichnis über Verarbeitungstätigkeiten und/oder eine Datenschutz-Folgeabschätzung gemäß den geltenden Gesetzen erstellen muss. In jedem Fall ist der Kunde als Erheber, Inhaber und Verwender der Daten der Verantwortliche im Sinne der EU-DSGVO. Die NewDefinition GmbH verarbeitet die Daten nicht und nimmt keine Änderungen an ihnen vor – es sei denn auf gesonderte schriftliche Weisung des Kunden. Sie speichert die Daten lediglich im Auftrag des Kunden und ermöglicht deren Verarbeitung im Rahmen der bereitgestellten Software.

4. Anzahl der Administratoren und Rechtevergabe

Die Anzahl der Administratoren sollte stets auf das „Notwendigste“ reduziert bleiben und temporäre Einzelrechte nur für die erforderliche Minimalzeit und in dem erforderlichen Minimnalumfang vergeben werden. Der Kunde ist für die Verwaltung der Administrationskonten und die Rechtevergabe selbst verantwortlich.

5. Abschluss einer Auftragsdatenverarbeitungsvereinbarung (ADV)

Die NewDefinition GmbH verarbeitet zwar die Daten ihrer Kunden und deren Nutzer/Mitglieder nicht, bietet aber die dazu notwendige Software nebst erforderlichen Nebenleistungen wie Hosting, Datensicherung etc. an und ist damit im Sinne der Gesetzgebung allein durch die Speicherung der Kundendaten ein Auftragsdatenverarbeiter/Auftragsverarbeiter. Für diesen Zweck ist neben dem Hauptvertrag (Anwendugnsdienstleistervertrag) zur Nutzung der Software zusätzlich eine Auftragsdatenverarbeitungsvereinbarung (ADV) abzuschließen. Die Vertragsformulierung obliegt dabei dem Auftraggeber.