dun & bradstreet

Dun & Bradstreet Austria GmbH

Technische und organisatorische Maßnahmen zum Datenschutz

Stand: Oktober 2021

Inhaltsverzeichnis

1. GELTUNGSBEREICH

Nach der Datenschutzgrundverordnung (DSGVO) hat der Verantwortliche sowie der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, zu treffen. Dieses Dokument beschreibt die Maßnahmen, die im Sinn von Artikel 32 DSGVO im Bereich der D&B-Unternehmensgruppe in Österreich getroffen sind (in diesem Dokument zusammenfassend „D&B" genannt), namentlich durch die Dun & Bradstreet Austria GmbH Jakov-Lind Straße 4/1, 1020 Wien.

2. MAßNAHMEN ZUR VERTRAULICHKEIT (ARTIKEL 32 ABS. 1 DSGVO)

2.1. Zutrittskontrolle

Die Zutrittskontrolle dient dazu, Unbefugten den Zutritt zu den technischen Anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Der Zutritt zu den D&B Geschäftsräumen wird durch Zugangskontrollen geregelt. Diese bestehen für die Mitarbeiter von D&B in erster Linie in elektronischen Schlüsseln, die – im Umfang der pro Schlüssel hinterlegten Zugriffsrechte – den Zugang zur Betriebsstätte erlauben.
Die Zugriffsrechte sind sowohl zeitlich (auf die erlaubte Nutzung an bestimmten Wochentagen und zu bestimmten Tageszeiten) als auch räumlich (auf bestimmte Teile der Betriebsstätte) den Befugnissen der Mitarbeiter angepasst.
Für Betriebsfremde wird die Zutrittskontrolle durch einen zentralen Empfang sichergestellt, der die Daten der Besucher erfasst. Diese werden zu jeder Zeit von einem Mitarbeiter von D&B begleitet bzw. während ihrer Tätigkeit beaufsichtigt.
Die IT-Systeme von D&B werden am Geschäftsstandort von D&B betrieben. Die Datacenter sind als geschlossener Sicherheitsbereich konzipiert. Es besteht sowohl baulicher als auch technischer Zugangsschutz. Die Datacenter sind elektronisch gesichert und Besucher erhalten nur in Begleitung Zutritt und werden nicht unbeaufsichtigt gelassen. Die für den Zutritt benötigten Zugänge werden nur nach vorheriger Anmeldung und unter engen Voraussetzungen ausgegeben. Die Nutzung wird protokolliert.
Die Ein- und Ausgänge zu den Geschäftsräumen werden außerhalb der Geschäftszeiten per Video und Alarmanlage überwacht und das Gelände sowie die kritischen Innenbereiche des Gebäudes werden außerdem durch einen Sicherheitsdienst überwacht.

2.2. Zugangskontrolle

Die Zugangskontrolle umfasst Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen (logische Sicherheit) durch Unbefugte verhindert wird.
Jeder Mitarbeiter von D&B hat seine eigenen persönlichen Zugangsdaten für seinen Rechner um Zugriff zu den Systemen bzw. Datenbanken zu bekommen.
Arbeiten an den D&B-Systemen werden nur von Mitarbeitern durchgeführt, die eine gesonderte Vertraulichkeitserklärung unterzeichnet haben und vor Einstellung überprüft wurden. Die Vertraulichkeitserklärung enthält eine Verpflichtung auf das Datengeheimnis nach § 6 Datenschutz-Anpassungsgesetz 2018. Erfolgen Tätigkeiten über externe Zugänge, sind diese sogenannten VPN-

Verbindungen nach dem Stand der Technik verschlüsselt und es ist eine zusätzliche Authentifizierung erforderlich. Die Identifikation mit Benutzernamen und sicherem Passwort ist obligatorisch.
Die IT-Systeme von D&B sind darüber hinaus durch Firewall-Technologien gegen Eingriffe von außen abgeschirmt. Die Firewall wird zentral durch die Konzernmutter Bisnode AB, Solna (Schweden) betrieben und betreut.

2.3. Zugriffskontrolle

Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
D&B hat interne Standards für den Umgang mit Berechtigungen definiert und dokumentiert. Diese sind im Dienstvertrag bzw. Mitarbeiter-Handbuch festgelegt (Geheimhaltung, Verbot von Weitergabe der Passwörter, etc.). Neue Mitarbeiter werden entsprechend auf den Umgang mit den Daten eingewiesen.
Die Vergabe von Benutzerzugängen ist ein standarisierter Prozess beim Eintritt ins Unternehmen. Diese werden dem Mitarbeiter telefonisch oder persönlich übergeben, nach dem ersten Login muss der Benutzer das Passwort ändern.
Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Groß- und Kleinbuchstaben sowie Zahlen müssen enthalten sein. Die Passwörter müssen per Windows Policy alle 60 Tage geändert werden und die letzten 8 Passwörter können nicht wiederholt gesetzt werden. Wird das Passwort nicht rechtzeitig geändert oder das Passwort wird 5-mal falsch eingegeben, wird der Benutzer automatisch gesperrt. Natürlich ist das selbstständige Ändern des aktuellen Passworts jederzeit möglich.
Über die Windows Group Policy wird auf jeden Rechner die automatische Sperre des Computers, bei Nichtverwendung nach 10 Minuten, eingestellt.
Zugriffsrechte auf Dateien werden über das Windows Active Directory verwaltet. Erweiterte Rechte müssen über einen Genehmigungsprozess über den jeweiligen Vorgesetzen und schriftlich in der IT beantragt werden.
Telearbeit wird auf von D&B zur Verfügung gestellten Computern durchgeführt. Die Verbindung zu D&B wird hier über einen zentral verwalteten VPN-Tunnel hergestellt.
Stationäre Laptops sind mit Kensington Locks gesichert, Mobile Mitarbeiter Laptops haben verschlüsselte Festplatten.
Die Zugriffsrechte auf File-Shares sind über Rollen/Gruppen realisiert, wo Abteilungsweise (bzw. Funktionsweise) auf die jeweiligen Shares zugegriffen werden kann.
Die Einzelheiten sind im „Rollen- und Berechtigungskonzept" von D&B geregelt.
Beim Austritt von Mitarbeitern werden sofort alle Zugänge zu den Systemen gesperrt. Sämtliche Unterlagen, ausgehändigte Schlüssel und IT-Geräte werden eingezogen.
Alte Datenträger und Sicherheitsbänder werden physisch zerstört.
Alle User in der Active Directory und deren Rechte im Netzwerk werden in regelmäßigen Abständen geprüft und gegeben falls geändert und angepasst.

2.4. Trennungskontrolle

Das Trennungsgebot umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Bezüglich der allgemeinen Verarbeitung ihrer Daten bei D&B (Mitarbeiterdaten, Lieferantendaten, Kundenstammdaten) wird das Trennungsgebot umgesetzt durch beispielsweise die physikalische Trennung und Speicherung auf gesonderten Systemen oder Datenträgern, Trennung von Produktiv-, Test- und Entwicklungsumgebung unserer Anwendungen und IT-Systeme, entsprechende Berechtigungskonzepte, sowie Datenbankrechten. Darüber hinaus wird softwareseitig eine logische Mandantentrennung umgesetzt.
Im Rahmen der geschäftsmäßigen Datenverarbeitung durch D&B, insbesondere den Empfang und die Bereitstellung von Daten ihrer Kunden im Rahmen des Auskunftsgeschäfts von D&B, erfolgt die Trennung im Sinne des Datenschutzes überwiegend auf Basis der Anwendung. Alle gelieferten Datenpakete werden strikt voneinander getrennt bearbeitet, so dass eine Überschneidung von Kundendaten ausgeschlossen ist. Hierzu sind die notwendigen Vorkehrungen (Hardware und Software) getroffen.

3. MAßNAHMEN ZUR INTEGRITÄT (ARTIKEL 32 ABS. 1 DSGVO)

3.1. Weitergabekontrolle

Die Weitergabekontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
Bezüglich der allgemeinen Verarbeitung ihrer Daten bei D&B (Mitarbeiterdaten, Lieferantendaten, Kundenstammdaten) wird die Weitergabekontrolle (Übertragungskontrolle, Transportkontrolle, Übermittlungskontrolle) gewährleistet durch entsprechend geeignete technische Maßnahmen.
Für die Datenübertragung an / von Kunden werden nur Übertragungsverfahren genutzt die eine Verschlüsselung der Daten ermöglichen (SFTP, VPN-Tunnel, Verschlüsselung mit PGP).
Die D&B Systeme sind durch einen Firewall-Cluster von anderen System isoliert und ein IPS-System (Intrusion Prevention) zur frühzeitigen Erkennung/Verhinderung von Einbruchsversuchen ist in Betrieb.
Backups die im Zuge des wöchentlichen Backup-Zyklus an eine externe IT-Sicherheitsfirma ausgehändigt werden, sind verschlüsselt und werden in einem verschlossenen Behälter übergeben.
Im Rahmen der geschäftsmäßigen Datenverarbeitung durch D&B, insbesondere den Empfang und die Bereitstellung von Daten ihrer Kunden im Rahmen des Auskunftsgeschäfts von D&B, wird die Weitergabekontrolle durch die Protokollierung sämtlicher Schritte der Datenverarbeitung gewährleistet. Falls mit dem Kunden vereinbart, werden als besonders vertraulich klassifizierte Daten bei der Übertragung über öffentliche Netze zusätzlich verschlüsselt. Daten ihrer Kunden, die D&B für den Kunden im Auftrag verarbeitet, werden entsprechend den gesetzlichen Regelungen zur Auftragsdatenverarbeitung (§ 28 DSGVO) nur nach schriftlicher Weisung des Kunden an Dritte weitergegeben.

3.2. Eingabekontrolle

Die Eingabekontrolle umfasst Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Eingabe kann nur durch die Mitarbeiter erfolgen, die Zugriff auf die Daten haben.
Zugriff auf die Recherchedaten sind nur während des Verarbeitungsprozesses gegeben. Es wird protokolliert welcher Mitarbeiter die Daten zu welchem Zeitpunkt verarbeitet hat.
Darüber hinaus werden automatisch Protokolle „bestimmter Aktionen" von Prozessen auf den Systemen erstellt. Die Protokolle der „bestimmten Aktionen" beziehen sich auf Prozesse, die der Aufrechterhaltung des Systembetriebs, Abrechnungszwecken und zur Erfüllung gesetzlicher Speicherpflichten dienen.

4. MAßNAHMEN ZUR VERFÜGBARKEIT UND BELASTBARKEIT (ARTIKEL 32 ABS. 1 DSGVO)

4.1. Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
D&B verfügt über redundante Versorgungssysteme mit unterbrechungsfreier Stromversorgung.
Weiters werden auch die zentralen Systeme in ein Ausfallrechenzentrum repliziert um im Disaster-Recovery schnellst möglich wieder verfügbar zu sein. Die Vorgehensweise sind in im Disaster-Recovery Plan dokumentiert.
Die D&B Systeme sind durch einen Firewall-Cluster von anderen System isoliert und ein Intrusion Prevention System zur frühzeitigen Erkennung/Verhinderung von Einbruchsversuchen ist in Betrieb.
Des Weiteren werden die Systemprogramme und Hardware regelmäßig durch Updates auf dem neuesten Stand gehalten. Ein zentrales Antivirus System und Email Spam Filter sind ebenfalls in Betrieb.
Darüber hinaus wird die Datenverfügbarkeit, insbesondere der Schutz vor Datenverlust durch technisches Versagen oder versehentliches Löschen, durch regelmäßige Datensicherungen und Backups des gesamten Systems und Daten erstellt, die in einem wöchentlichen Zyklus bei einer externen IT-Sicherheitsfirma gelagert werden.
Weiters ist ein Überwachungs-Tool in Betrieb, das die Server und Applikationen von D&B ständig prüft und gegebenen falls Alarm schlägt und auf eventuelle Probleme so früh wie möglich zu reagieren.
Das Rechenzentrum ist baulich getrennt und nur über Schlüsselzugänge betretbar. Eine redundante Klimaanlage kühlt die Systeme im Raum. Rauchmelder und Sensoren für Temperatur und Wassereintritt sind in Betrieb.
Personenbezogene Daten speichert D&B solange, wie es zur Leistungsabwicklung erforderlich ist. Danach werden sie gelöscht, es sei denn, ihre – zweckgebundene – weitere Speicherung ist notwendig zur Erfüllung handels- und steuerrechtlicher Aufbewahrungspflichten oder zur Erhaltung von Beweismitteln im Rahmen der gesetzlichen Verjährungsvorschriften.

5. MAßNAHMEN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ARTIKEL 25 ABS. 1 DSGVO)

5.1. Datenschutz-Management

Das Datenschutz-Management beschreibt die innerbetrieblichen Maßnahmen für die besonderen Anforderungen des Datenschutzes.

	Maßnahmen
01	Bei D&B ist ein betrieblicher Datenschutzbeauftragter bestellt.
02	Es gibt bei D&B einen Beauftragten für die IT-/Informationssicherheit.
03	Es existieren Vertretungsregelungen für die DV-Verantwortlichen (Verantwortlich für die eingesetzte IT-Infrastruktur des Auftragnehmers) bei D&B.
04	Die Beauftragten für IT-/Informationssicherheit und Datenschutz bei D&B sind angemessen ausgebildet und verfügen über ein angemessenes fachliches Know-how und eine angemessene persönliche Eignung.
05	Die Beauftragten für IT-/Informationssicherheit und Datenschutz des Auftragnehmers sind angemessen in die Organisationsstruktur eingebunden (als Stabsstelle zur Organisationsleitung oder in vergleichbar unabhängiger Position).
06	Es finden regelmäßige Basisschulungen der Mitarbeiter zu Informationssicherheit und Datenschutz statt.
07	Es existieren Prozesse zur regelmäßigen Bewertung und Aktualisierung des Schulungsangebots an das erforderliche Niveau und an stattgefundene Änderungen in den Anforderungen oder Rahmenbedingungen (Änderung der Gesetze, neue Gesetze und Vorschriften).
08	Die Mitarbeiter, die mit personenbezogenen Daten zu tun haben, werden auf den Datenschutz und den befugten Umgang unterwiesen bzw. verpflichtet.
09	Es existiert eine übergeordnete Richtlinie/Policy zum Datenschutz.
10	Es existiert eine übergeordnete Richtlinie/Policy zur IT-Sicherheit.
11	Diese Richtlinien sind zentral abgelegt und allen Mitarbeitern zugänglich.
12	Die Vorgaben aus diesen Richtlinien sind in den Arbeitsanweisungen u.Ä. berücksichtigt.
13	Es existieren dokumentierte Prozesse zur Identifizierung, Analyse, Bewertung und Berücksichtigung von Änderungen in den Anforderungen (z.B. Datenschutzgesetze) sowie den IT-Verfahren und Prozessen (Datenschutzfolgenabschätzung, neue Anwendungen, neue IT-Systeme etc.).
14	Es existieren dokumentierte Prozesse zur Identifizierung, Analyse, Bewertung von Datenschutzvorfällen im Zuge von Änderungen sowie der Ableitung von Maßnahmen zur Verhinderung eines erneuten Eintritts (Verbindung des Change-Managements zum Incident-Management).

5.2. Incident-Response-Management

D&B ist sich der gesetzlichen Meldepflichten bewusst und hat seine Mitarbeiter sensibilisiert und trainiert, etwaige meldepflichtige Verstöße zu erkennen. Es ist ein entsprechender Meldeprozess, definierte. Den Adressaten der Meldung (Kundenservice) und den Mitarbeitern ist bekannt, an wen sie sich im Falle einer Datenschutzverletzung wenden müssen. Es ist weiterhin ein Prozess zur umgehenden Bearbeitung nach Eingang der Meldung umgesetzt. Die Mitglieder des „Krisenstabs" sind definiert und die Bewertung des Vorfalls sowie gegebenenfalls Auslösung der Meldung ist gewährleistet.
Das Incident Response Management für Datenschutzvorfälle ist verbunden mit dem IT-Incident Management, Security Incident Management, Notfall- bzw. Krisenmanagement der Bisnode AB.

5.3. Datenschutzfreundliche Voreinstellungen

Zur Umsetzung des Artikel 25 Abs. 2 DSGVO hat D&B eine „Group Privacy by Design & Default Guideline" erstellt. Diese regelt, dass D&B proaktiv und nicht reaktiv Datenschutz in alle Bereiche einbindet und Datenschutz bereits in der Design-Phase von Angeboten berücksichtigt wird. Privacy by Design-Compliance ist für D&B nicht nur eine Frage von User-Experience. Zu einer angemessene Compliance gehören auch, angemessene technische und sicherheitstechnische Maßnahmen zum Schutz der Benutzerdaten und personenbezogenen Daten zu ergreifen.
Des Weiteren hat D&B eine „Group Retention Policy" erstellt. Dabei handelt es sich um ein Basisdokument, das in jedem Markt mit lokalen Abweichungen separat realisiert ist. Hierzu hat die D&B in Österreich ein entsprechendes Löschkonzept für personenbezogene Daten umgesetzt.

5.4. Auftragskontrolle

Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
Sofern D&B personenbezogene Daten im Auftrag verarbeitet, wird dazu stets ein schriftlicher Vertrag zur Auftragsdatenverarbeitung mit dem gemäß § 28 Abs. 9 DSGVO gesetzlich erforderlichen Inhalt abgeschlossen. D&B hält für diesen Fall auch eigene Vertragsmuster vor, die der Auftraggeber für die Beauftragung verwenden kann.
Durch vertragliche Verpflichtungen ist sichergestellt, dass D&B die Daten des Auftraggebers nur nach dessen Weisungen verarbeitet, die Vertraulichkeit der Daten zu gewährleisten ist und insbesondere ohne ausdrückliche anderslautende Anweisung des Kunden keine Übernahme von Kundendaten in den allgemeinen Auskunftsdatenbestand von D&B stattfindet.
Darüber hinaus sind die Beschreibungen zu den technischen und organisatorischen Schutzmaßnahmen bei D&B Bestandteil jeden Auftragsdatenverarbeitungsvertrags mit D&B, indem dieses Dokument als Anlage zum Auftragsdatenverarbeitungsvertrag vereinbart wird.

Dun & Bradstreet Austria GmbH
Oktober 2021