Verzeichnis der Verarbeitungstätigkeiten

Technisch und organisatorische Maßnahmen i.S.d. Art. 32 EU-DSGVO

Grundsätzliches

In Deutschland sind alle Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten oder nutzen, gesetzlich verpflichtet, die erforderlichen und angemessenen technischen und organisatorischen Maßnahmen zum Erzielen und Aufrechterhalten der Datensicherheit zu treffen. Dies ergibt sich insbesondere aus Art. 32 DSGVO.

Der Anforderungskatalog listet eine Reihe von Maßnahmen auf, um das Ziel Datensicherheit zu erreichen. Die gesetzlichen Anforderungen an die erforderlichen Datensicherungsmaßnahmen sind im Gesetz jedoch flexibel gehalten, da sie u.a. unabhängig von einem bestimmten Stand der Technik und verwendeten Medien beschrieben werden.

Generell gilt, dass sich die zu treffenden Maßnahmen an den zu schützenden Unternehmenswerten zu orientieren haben. Hierfür bietet sich zunächst die Durchführung einer Schutzbedarfsanalyse als Grundlage eines Sicherheitskonzepts an, um zu ermitteln, welcher Schutz für die Informationen und die eingesetzte Informationstechnik erforderlich sowie angemessen ist.

Das Unternehmen Bund-Verlag GmbH, Emil-von-Behring-Str. 14, 60439 Frankfurt am Main erfüllt diesen Anspruch durch folgende Maßnahmen.

Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☒ Schlüsselverwaltung / Dokumentation der Schlüsselvergabe(Chips)
☐ Automatisches Zugangskontrollsystem	☐ Empfang / Rezeption
☐ Biometrische Zugangssperren	☐ Pförtner / Werkschutz
☒ Chipkarten / Transpondersysteme	☐ Besucherbuch / Protokoll der Besucher
☐ Manuelles Schließsystem	☐ Mitarbeiter- / Besucherausweise
☐ Sicherheitsschlösser	☐ Besucherregelung / Begleitung durch Mitarbeiter / Besucherausweis
☒ Elektronische Türöffner teilweise	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☒ Bewachung außerhalb der Betriebszeiten
☐ Absicherung der Gebäudeschächte	☒ Sorgfalt bei Auswahl Reinigungsdienste

Verzeichnis der Verarbeitungstätigkeiten

Technisch und organisatorische Maßnahmen i.S.d. Art. 32 EU-DSGVO

☒ Türen mit Knauf Außenseite	☐ Sperrbereiche
☒ Generalschlüssel	
☐ Klingelanlage mit Kamera	
☒ Videoüberwachung der Eingänge Im Serverraum	
☐ Vergitterte Fenster/Türen	
☐ Zaunanlagen	
☒ Spezielle Schutzvorkehrungen Serverraum Videoüberwachung im Serverraum	
☒ Spezielle Schutzvorkehrungen Backups	

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von Call-Back-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Zentrale Verwaltung von Benutzerberechtigungen
☒ Login mit biometrischen Daten Anmeldung Tablet, Handy, einzeln verwaltet durch den MA	☒ Autorisierungsprozess für Zugangsberechtigungen
☒ Single Sign-On teilweise	☒ Erstellen von Benutzerprofilen
☐ Zwei-Faktor-Authentifizierung (TAN, Token, Chipkarten, etc.)	☒ Zentrale Passwortvergabe
☒ Anti-Viren-Software Server Kaspersky	☒ sichere Dokumentation und Aufbewahrung der Passwörter
☒ Anti-Virus-Software Clients s.o.	☒ Richtlinie „Sicheres Passwort“
☒ Anti-Virus-Software mobile Geräte Kaspersky- in der Einführung	☒ Richtlinie „Löschen / Vernichten“
☒ Firewall Watch Guard, Windows/Linux Firewall	☒ Richtlinie „Clean desk“

☒ Intrusion Detection/Prevention Systeme s.o.	☒ Allg. Richtlinie zur IT-Sicherheit
☒ Mobile Device Management Kaspersky-in der Einführung	☒ Mobile Device Policy BV
☒ Einsatz VPN bei Remote-Zugriffen	☒ Anleitung „Manuelle Desktopsperre“
☒ Verschlüsselung von Datenträgern Notebooks	☒ Begrenzung der Anzahl befugter Benutzer
☐ Verschlüsselung Smartphones	☒ Kennwortverfahren (regelmäßige Änderungen)
☐ Gehäuseverriegelung	
☐ BIOS Schutz (separates Passwort) Ggf. in der Einführung	
☐ Sperre externer Schnittstellen (USB)	
☒ Automatische Desktopsperre	
☒ Verschlüsselung von Notebooks / Tablet	
☒ Nicht-reversible Vernichtung von Datenträgern	

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Zugriffskontrolle

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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenshredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte (differenzierte Berechtigungen)
☒ Externer Aktenvernichter (DIN 66399, alt: 32757)	☒ Minimale Anzahl an Administratoren
☒ Physische Löschung von Datenträgern	☒ Datenschutztresor

☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten teilweise	☒ Verwaltung Benutzerrechte durch Administratoren
☒ Verschlüsselung von CD/ DVD, externen Festplatten und/ oder Laptops	☐ Auswertungen von Datenverarbeitungen
☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbaren Datenträger	☒ Autorisierungsprozess für Berechtigungen
☒ Mobile Device Management-System	☒ Genehmigungsroutinen (Zeichnungsrichtlinie)
☒ Nicht-reversible Löschung von Datenträgern	☒ Profile/ Rollen
☒ Sichtschutzfolien für öffentliche/mobile Bildschirme Personalbereich	☒ Vier-Augen-Prinzip
	☐ Funktionstrennung „Segregation of Duties“

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	☒ Datensätze sind mit Zweckattributen versehen

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Verzeichnis der Verarbeitungstätigkeiten

Technisch und organisatorische Maßnahmen i.S.d. Art. 32 EU-DSGVO

Technische Maßnahmen	Organisatorische Maßnahmen
☐ getrennte Speicherung von Zusatzinformationen zur Identifikation	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
☐ Verschlüsselung von Zusatzinformationen zur Identifikation	☒ Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation
☐ Kopierschutz hinsichtlich Zusatzinformationen zur Identifikation	☐ Autorisierungsprozess oder Genehmigungsroutinen für Berechtigungen auf die Zusatzinformationen zur Identifikation
	☐ Vier-Augen-Prinzip für Identifikation

Weitere Maßnahmen:

Es findet keine Pseudonymisierung statt.

Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones s.o. teilweise	☒ Verschlüsselte Aufbewahrung von Passwörtern
☒ Verschlüsselung von mobilen Speichermedien (CD/DVD, USB-Stick, externen Festplatten) mobile Speichermedien selten benutzt	☒ Verschiedene Passwörter zur Verschlüsselung
☐ Verschlüsselung von Dateien	
☐ Verschlüsselung von Systemen/ Anlagen	
☐ Verschlüsselung von E-Mail und E-Mail-Anhängen	
☒ Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)	
☒ Gesichertes WLAN	

Weitere Maßnahmen:

Es findet keine Verschlüsselung statt.

Verzeichnis der Verarbeitungstätigkeiten

Technisch und organisatorische Maßnahmen i.S.d. Art. 32 EU-DSGVO

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Email-Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der -Löschfristen
☒ Einsatz von VPN	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐ Protokollierung der Zugriffe und Abrufe Logfiles Implementierung der Auditing in der Prüfung	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☐ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐ Persönliche Übergabe mit Protokoll
☐ Nutzung von Signaturverfahren	☒ Zugriffsrechtekonzept

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten Logfiles Bund online, NTX, easy Archiv	☐ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können

☐ Manuelle oder automatisierte Kontrolle der Protokolle	☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☒ Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☐ Serverraumüberwachung Temperatur und Feuchtigkeit wird eingeführt	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Schutzsteckdosenleisten Serverraum	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☒ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ RAID System / Festplattenspiegelung	
☒ Videoüberwachung Serverraum	

☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

Weitere Maßnahmen:

Keine weiteren Maßnahmen.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösungen für Datenschutz-Management im Einsatz	☒ Interner / externer Datenschutzbeauftragter consileo GmbH & Co. KG
☐ Zentrale Dokumentation aller Verfahrens-weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☐ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
☒ Anderweitiges dokumentiertes Sicherheits-Konzept	☐ Interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt
☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☒ Die Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Weitere Maßnahmen:

Informationssicherheitsbeauftragter in Planung.

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Verzeichnis der Verarbeitungstätigkeiten

Technisch und organisatorische Maßnahmen i.S.d. Art. 32 EU-DSGVO

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von ☒ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Intrusion Prevention System (IPS)	☐ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Weitere Maßnahmen:

Keine weiteren Maßnahmen vorhanden.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy-by-design / Privacy-by-default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ der Datenschutzbeauftragte wird in neue Prozesse zur Verarbeitung personenbezogener Daten frühestmöglich eingebunden.
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen vgl. arbeitrecht.de Prüfung der Einführung der Selbstlöschung vgl. nextcloud	

Verzeichnis der Verarbeitungstätigkeiten

Technisch und organisatorische Maßnahmen i.S.d. Art. 32 EU-DSGVO

Weitere Maßnahmen: -

Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Organisatorische Maßnahmen
☐ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
☐ Schriftliche Weisungen an den Auftragnehmer
☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐ Regelung zum Einsatz weiterer Subunternehmer
☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen:

Keine weiteren Maßnahmen.