No.	Merkmal	Verarbeitungstätigkeit 1	Verarbeitungstätigkeit 2	Verarbeitungstätigkeit 3	Verarbeitungstätigkeit 4	Verarbeitungstätigkeit 5	Verarbeitungstätigkeit 6	Verarbeitungstätigkeit 7	Verarbeitungstätigkeit 8	Verarbeitungstätigkeit 9
1	Verarbeitungstätigkeit	Zeiterfassung	Patchmanagement (intern)	Patchmanagement (extern)	Firewalladministration	Administration E-Mail System	Administration Ressourcenverwaltung (elektronisch)	Benutzerverwaltung und Zugriffsberechtigungen IT und TK-Anlage	Datensicherungsmanagement	Administration Netzwerke (inkl. Internet)
2	Fachverantwortlicher Ansprechpartner	User Online Bearbeiten	User Online Bearbeiten	User Online Bearbeiten	User Online Bearbeiten	User Online Bearbeiten	User Online Bearbeiten	User Online Bearbeiten	User Online Bearbeiten	User Online Bearbeiten
3	Zweck der Verarbeitung	Erfassung der Arbeitszeiten der einzelnen Mitarbeiter zur Erfüllung der Nachweispflicht, bzw Führung der Arbeitszeitkonten, Erfassung von Urlaubs- und Krankheitstagen	selbst durchgeführte Aktualisierung der eingesetzten Softwareprodukte (Patches, Updates, etc.)	extern durchgeführte Aktualisierung der eingesetzten Softwareprodukte (Patches, Updates, etc.)	Administration der Firewall (Erlaubnis oder Verhinderung von Zugriffen basierend auf IP-Adressen)	Die IT administriert das E-Mail-System. Sie hat daher theoretisch Zugriff auf alles was dort verarbeitet wird. Dazu gehört des Versenden / Empfang von E-Mails und Telefaxe, Terminverwaltung, Adressverwaltung. Der E-Mail-Versand und -Empfang werden protokolliert. Diese Protokolle werden bei Bedarf von der Abteilung Informationstechnik analysiert (z. B. bei hohem SPAM-Aufkommen von einer bestimmten Domain). System ist nur von intern zu erreichen.	Die Ressourcen in der Verwaltung (z. B. Raumplanung, KFZ-Bestellung, Dienstfahrzeuge, etc.) werden elektronisch verwaltet. Die Planung ist grundsätzlich für jeden Mitarbeitenden einsehbar (über einen für die Mitarbeitenden öffentlichen Kalender), auch um die Abstimmung zu erleichtern. System ist nur von intern zu erreichen.	Verwaltung von Benutzern und Zugriffsberechtigungen im Active Directory Verzeichnis und in Fachverfahren, die Zugriffsberechtigungen werden auf Anweisung der Vorgesetzten des Betroffenen eingestellt.	Die Daten der Verwaltung werden regelmäßig und anlassbezogen gesichert um Datenverluste durch z. B. Virenbefall zu minimieren. Gegenstand der Datensicherung sind alle Daten auf den Netzlaufwerken. Nach erfolgter Sicherung werden die Daten archiviert.	Die Verwaltung betreibt verschiedene Netze, die unterschiedlich abgesichert sind. Die IT hat die Aufgabe dafür zu sorgen, dass diese Netze vorneinander getrennt und wie vorgesehen funktionieren. Des Weiteren wird die Nutzung protokolliert.
4	Verarbeitete personenbezogene Daten	- Name, - Personalnummer, - Adresse	- ggf. IP-Adressen, - ggf. Inhalte von Protokollen, - ggf. Benutzeraktivitäten und/oder -Rechte	- ggf. IP-Adressen, - ggf. Inhalte von Protokollen, - ggf. Benutzeraktivitäten und/oder -Rechte	- IP-Adressen	- Inhalte von E-Mails, - Absender, - Empfänger	- Inhalte von Buchungen, - Antragsteller	- Name, - Nutzerkennung, - berufliche Position, - E-Mail Adresse	- Alle Daten die auf den Netzlaufwerken abgelegt werden.	- IP-Adresse, - Kennung
5	Besondere personenbezogene Daten	Keine besonderen personenbezogenen Daten	Keine besonderen personenbezogenen Daten	Keine besonderen personenbezogenen Daten	Keine besonderen personenbezogenen Daten	Abhängig von der E-Mail	Keine besonderen personenbezogenen Daten	Keine besonderen personenbezogenen Daten	Alle Daten die auf den Netzlaufwerken abgelegt werden.	Keine besonderen personenbezogenen Daten
6	Betroffene Personen	- Beamte, - Beschäftigte, - Auszubildende	- Mitarbeitende (wenn Patchstände und/oder Inhalte von Protokollierungen eingesehen werden können)	- Mitarbeitende (wenn Patchstände und/oder Inhalte von Protokollierungen eingesehen werden können)	- Mitarbeitende	- E-Mail-Nutzer (sowohl intern als auch extern)	- Antragsteller, - Nutzer der elektronischen Ressourcenverwaltung	- Mitarbeitende	- Mitarbeitende, -Personen deren Daten auf den Netzlaufwerken der Verwaltung verarbeitet werden	- Mitarbeitende, - Nutzer der Gastnetze (z. B. WLAN)
7	Datenempfänger *intern (wer erhält die Daten?)*	- Vorgesetzte der Betroffenen, - ggf. Personal	- IT-Administratoren	- IT-Administratoren	- N/A	- Betroffene	- alle Mitarbeitenden	- Abteilungsleitungen	- Archiv	- N/A
8	Datenempfänger *extern (wer erhält die Daten?)*	N/A	- N/A	- Mitarbeitende von IT-Dienstleistern	- ggf. Support Dienstleister!	- Betroffene	- N/A	- N/A	- ggf. Dienstleister für Archivierung (z. B. Bank)	- N/A
9	Übermittlung an Nicht-EU-Länder?	Findet nicht statt	Findet nicht statt	Findet nicht statt	Findet nicht statt	Findet nicht statt	Findet nicht statt	Findet nicht statt	Findet nicht statt	Findet nicht statt
10	*falls ja, in welche und warum?*									
11	Findet Profiling statt?	Findet nicht statt	Findet nicht statt	Findet nicht statt	Findet statt	Findet statt	Findet nicht statt	Findet nicht statt	Findet nicht statt	Findet nicht statt
12	*falls ja, wonach und warum?*				Verwaltung sperrt Verbindungsversuche basierend auf stetig aktualisierter Blacklist	Verdächtige E-Mails werden blockiert bzw. unter Quarantäne gestellt				
13	Verarbeitungsgrundlage	Vertrag (Art. 6 (1) lit. b)	Öffentliches Interesse (Art. 6 (1) lit. e)	Vertrag (Art. 6 (1) lit. b)	Öffentliches Interesse (Art. 6 (1) lit. e)	Öffentliches Interesse (Art. 6 (1) lit. e)	Öffentliches Interesse (Art. 6 (1) lit. e)	Öffentliches Interesse (Art. 6 (1) lit. e)	Öffentliches Interesse (Art. 6 (1) lit. e)	Öffentliches Interesse (Art. 6 (1) lit. e)
14	*falls rechtlich, Gesetz & Paragraph angeben*									
15	Löschfristen *(Frist und rechtliche Grundlage angeben)*	- 5 Jahre (§GZG)	- N/A (personenbezogene Daten werden nur gespeichert wenn dies zur Aufklärung eines Problems oder Vorgangs notwendig ist)	-N/A (personenbezogene Daten werden nur gespeichert wenn dies zur Aufklärung eines Problems oder Vorgangs notwendig ist)	- 2 Monate (bei Verdachtsmomenten bzw. laufenden Ermittlungen auch länger)	- Protokolle: 3 Monate (bei Verdachtsmomenten bzw. laufenden Ermittlungen auch länger). - Die E-Mails selbst werden von den jeweiligen Empfängern N/Abwandern verwaltet und ggf. gelöscht	- Protokolle: 3 Monate (bei Verdachtsmomenten bzw. laufenden Ermittlungen auch länger)	- Bei Ausscheiden aus dem aktiven Beschäftigungs- oder Dienstverhältnis oder einem Wechsel der eine Veränderung der Zugriffsberechtigungen bedingt (es wird stets nur der aktuelle Status der Benutzerverwaltung nachgehalten, keine historischen Zustände)	- N/A, für die Datensicherungen gelten keine eigenen Löschfristen, stattdessen ist dies von den jeweils gesicherten Daten abhängig	- Protokolle: 3 Monate (bei Verdachtsmomenten bzw. laufenden Ermittlungen auch länger).
16	Welche(s) Fachverfahren wird/werden genutzt? *(Name und Verzeichnis angeben)*	ZEITIME	kein Fachverfahren	kein Fachverfahren	kein Fachverfahren	Outlook	kein Fachverfahren	kein Fachverfahren	kein Fachverfahren	kein Fachverfahren
17	Allgemeine Beschreibung technisch-organisatorischer Maßnahmen.	Zugriffsbeschränkung	s.A.	s.A.	s.A.	s.A.	s.A.	s.A.	s.A.	s.A.