Checkliste zum Datenschutz in der Personalabteilung

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de

Maßnahmen zum Personaldatenschutz

Bitte beachten Sie, dass die folgende Liste nicht abschließend ist und nur beispielhafte Maßnahmen für den Beschäftigtendatenschutz enthält.

Maßnahme / Prüfpunkt	Status		
	Erledigt	In Bearbeitung	Offen
Umgang mit Bewerbungen und personenbezogenen Daten von Bewerben			
Haben Sie eine separate E-Mail-Adresse für Bewerbungen eingerichtet?			
Ist sichergestellt, dass nur autorisierte Mitarbeiter der Personalabteilung auf das Postfach und die Bewerbungsunterlagen zugreifen können?			
Haben Sie Standardantworten für eingehende Bewerbungen eingestellt, um Ihre Informationspflichten gegenüber den Bewerben zu erfüllen?			
Ist in Ihrer Datenschutzerklärung ein Passus zu Bewerbungen enthalten?			
Bewahren Sie Bewerbungsunterlagen ordnungsgemäß und vernichten diese datenschutzkonform nach Ablauf der Aufbewahrungsfrist?			
Erheben Sie die Einwilligung der betroffenen Bewerber, wenn Sie die Bewerbungsunterlagen über einen längeren Zeitraum in den Bewerber-Pool aufnehmen wollen?			
Onboarding und Offboarding von Mitarbeitern			
Onboarding			
Liegt ein unterschriebener Arbeitsvertrag vor?			
Wurde der neue Mitarbeiter zur Vertraulichkeit und zur Einhaltung des Datenschutzes verpflichtet?			
Wurde der Mitarbeiter darüber informiert, wie bei Datenschutzverstößen oder Betroffenenanfragen vorzugehen ist?			
Wurde dem neuen Mitarbeiter die Kontaktdaten des Datenschutzbeauftragten bekannt gegeben?			
Falls Fotos des Mitarbeiters veröffentlicht werden sollen: Liegt hierzu eine schriftliche Einwilligung des Mitarbeiters vor?			
Falls interne Unternehmensrichtlinien mit Datenschutzrelevanz bestehen: Wurde diese dem Mitarbeiter vorgelegt?			
Offboarding			
Hat der ausscheidende Mitarbeiter die Möglichkeit erhalten, private Mails und Dateien von seinen Dienstgeräten zu löschen?			
Hat der Mitarbeiter die Firmenhardware zurückgegeben und würde die Rückgabe dokumentiert?			

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de

Wurde der E-Mail-Account des Mitarbeiters deaktiviert bzw. wurde das Passwort für den Account geändert und eine Weiterleitung der Mails eingerichtet?			
Wurden dem Mitarbeiter sämtliche Zugangsrechte entzogen (sowohl digital als auch physisch)?			
Wurden veröffentlichte Fotos des Mitarbeiters entfernt?			
Werden die Daten von ausgeschiedenen Mitarbeitern gemäß den gültigen Fristen aufbewahrt und nach Ablauf der Aufbewahrungsfrist datenschutzkonform vernichtet?			
Vertraulichkeitsvereinbarungen für Mitarbeiter			
Werden Mitarbeiter zur Einhaltung des Datenschutzes verpflichtet?			
Werden Mitarbeiter zur Einhaltung sonstiger Verschwiegenheiten verpflichtet (z.B. Vertraulichkeitsvereinbarung zum Geschäftsgeheimnis, Sozialgeheimnis, Fernmeldegeheimnis)?			
Umgang mit digitalen und analogen Personalakten			
Ist die Vertraulichkeit personenbezogener Daten in digitalen und analogen Personalakten durch definierte Zugriffsrechte gewährleistet?			
Können nur befugte Personen mit Personalverantwortung auf die Personalakten zugreifen?			
Werden Papierakten in einem abschließbaren Aktenschrank aufbewahrt, zu dem nur autorisierte Mitarbeiter Zugang haben?			
Sind digitale HR-Systeme und Datenbanken mit Passwörtern geschützt und die Zugriffsberechtigungen nur bestimmten Mitarbeitern zugeteilt?			
Ist die Verfügbarkeit der Daten auch in Notsituationen sichergestellt?			
Werden Papierakten in sicheren Räumen aufbewahrt, die auch brandschutztechnisch abgesichert sind?			
Existieren etablierte Löschroutinen für das datenschutzkonforme Löschen von Daten?			
Wird bei der Vernichtung von papiergebundenen Personalakten die datenschutzkonforme Aktenvernichtung beachtet, beispielsweise durch den Einsatz eines geeigneten Schredders oder eines externen Dienstleisters?			
Veröffentlichung von Mitarbeiterfotos			
Wird die ausdrückliche Einwilligung der Mitarbeiter für die Veröffentlichung ihrer Fotos eingeholt?			
Wird die Einwilligung spezifisch für jeden einzelnen Veröffentlichungskanal eingeholt?			
Wird die Einwilligung vor der Veröffentlichung der Fotos eingeholt?			

Hat der Mitarbeiter die Möglichkeit, seine Einwilligung jederzeit zu widerrufen?			
Wird in bestimmten Fällen das berechtigte Interesse des Unternehmens als Rechtsgrundlage herangezogen?			
Wird die Verwendung des berechtigten Interesses sorgfältig abgewogen und dokumentiert?			
Datenschutzrichtlinien im Unternehmen			
Werden für die gängigsten Prozesse im Unternehmen Arbeitsanweisungen zum Datenschutz erstellt?			
Sind in den Arbeitsanweisungen die datenschutzrelevanten Punkte schriftlich festgehalten?			
Existiert eine schriftliche Regelung für die Privatnutzung des dienstlichen Internetzugangs und E-Mail-Systems?			
Gibt es eine Clean-Desk-Richtlinie im Unternehmen?			
Sind Regelungen für die Arbeit aus dem Homeoffice festgelegt?			
Fuhrparkmanagement			
Wird die Fahrerlaubnis der Mitarbeiter, die Firmenfahrzeuge nutzen, regelmäßig geprüft?			
Wird bei der Kontrolle von Führerscheinen auf das Anfertigen von Kopien verzichtet und stattdessen eine Vor-Ort-Prüfung durchgeführt?			
Wird die Durchführung und das Ergebnis der Vor-Ort-Prüfung von Führerscheinen dokumentiert?			
Werden angefertigte Kopien von Führerscheinen regelmäßig gelöscht, nachdem eine neue Überprüfung stattfindet?			
Wird die Verwendung von GPS-Systemen in Firmenfahrzeugen klar kommuniziert und ausschließlich für betriebliche Zwecke eingesetzt?			
Wird Mitarbeitern empfohlen, bei der Nutzung von Pool-Fahrzeugen keine persönlichen Daten wie das Kontaktbuch ihres Handys mit dem Fahrzeug zu synchronisieren?			
Ist geregelt, dass Navigationsdaten nach jeder Nutzung von Pool-Fahrzeugen gelöscht werden, um die Privatsphäre der Fahrer zu schützen?			
Öffentliche Telefon- und Geburtstagslisten			
Wird die Einwilligung der Mitarbeiter eingeholt, bevor ihre Telefonnummern oder Geburtstage veröffentlicht werden?			
Wird der Zugang zu den veröffentlichten Listen streng kontrolliert, um Einsicht durch unbefugte Dritte zu verhindern?			
Werden die Listen nicht in für Kunden öffentlich zugänglichen Bereichen ausgehängt?			
Beschränken sich die in den Listen enthaltenen Daten auf das absolut Notwendige?			

Werden die Listen regelmäßig daraufhin überprüft, ob die enthaltenen Daten noch aktuell und notwendig sind?			
Werden Daten von ausgeschiedenen Mitarbeitern oder von Mitarbeitern, die ihre Einwilligung zur Veröffentlichung widerrufen, aus den Listen entfernt?			
Einrichtung und Ausstattung des Personalbüros			
Verfügt das Personalwesen über ein eigenes, abschließbares Büro, zu welchem nur Mitarbeiter des Personalwesens Zugang haben?			
Bietet das Personalbüro einen geeigneten Raum für vertrauliche Personalgespräche oder Telefonate?			
Sind die technischen Geräte im Personalbüro mit ausreichendem Passwortschutz eingerichtet?			
Sind die Schreibtische im Personalbüro so ausgerichtet, dass ein Sichtschutz für Bildschirme und Geräte gewährleistet ist?			
Sind die Bildschirme im Personalbüro mit Sichtschutzfolien versehen?			
Verfügt das Personalbüro über einen eigenen Drucker und einen datenschutzkonformen Schredder für die HR-Abteilung?			
Werden die Personalakten in Papierform in abschließbaren Schränken aufbewahrt, für die nur die Personalverantwortlichen einen Schlüssel haben?			
Datenschutz im Homeoffice			
Wird vor Beginn der Tätigkeit im Homeoffice eine Risikoanalyse durchgeführt, um Datenschutzrisiken abzuschätzen?			
Werden geeignete Schutzmaßnahmen getroffen, um die identifizierten Datenschutzrisiken im Homeoffice zu minimieren?			
Ist das Homeoffice im Arbeitsvertrag geregelt oder wird eine Zusatzvereinbarung zum Vertrag geschlossen?			
Existieren klare Homeoffice-Richtlinien, die jedem Mitarbeiter die Datenschutzregeln im Homeoffice vermitteln?			
Betreffen die vom Arbeitgeber vorgegebenen Schutzmaßnahmen auch Aspekte des Arbeitsschutzes?			
Werden praktische Checklisten zur Einhaltung des Datenschutzes und Arbeitsschutzes im Homeoffice angeboten?			
Datenaustausch im Konzern			
Darf Ihr Unternehmen die Daten Ihrer Beschäftigten an andere Stellen oder Unternehmen im Konzern weitergeben bzw. besteht hierzu eine rechtsgültige Grundlage?			
Wird das berechtigte Interesse als Rechtsgrundlage für den Datenaustausch innerhalb des Konzerns herangezogen?			
Werden bei der Nutzung des berechtigten Interesses die Interessen der betroffenen Mitarbeiter sorgfältig abgewogen?			
Finden Datenübermittlungen in Drittstaaten statt und wie wird dabei das Datenschutzniveau gewährleistet (z.B. durch Standardvertragsklauseln)?			

Datenschutz bei einer HR-Software			
Wird für die HR-Software ein Anbieter aus der EU gewählt, um die Einhaltung der DSGVO zu gewährleisten?			
Wird vor der Einführung der HR-Software eine Datenschutz-Folgenabschätzung durchgeführt?			
Wird der Datenschutzbeauftragte in den Prozess der Datenschutz-Folgenabschätzung einbezogen?			
Wird mit dem Anbieter der HR-Software ein Auftragsverarbeitungsvertrag abgeschlossen?			
Enthält der Auftragsverarbeitungsvertrag Klauseln über die technischen und organisatorischen Maßnahmen (TOMs) zur Gewährleistung der Datensicherheit?			
Ist sichergestellt, dass nur die notwendigen Personen im Unternehmen Zugriffsrechte für die HR-Software erhalten?			
Werden die Mitarbeiter transparent über den Einsatz der HR-Software und die damit verbundene Datenverarbeitung informiert?			
Datenschutz bei einer ausgelagerten Personalabteilung			
Wird sichergestellt, dass die Daten Ihrer Mitarbeiter auch bei einer ausgelagerten Personalabteilung datenschutzkonform behandelt werden?			
Werden bei der Auslagerung von HR-Aufgaben die gleichen Datenschutzregelungen wie beim Einsatz einer HR-Software (siehe oben) beachtet?			
Datenschutzschulung und Sensibilisierung der Mitarbeiter			
Sorgt der Arbeitgeber dafür, dass seine Angestellten die Datenschutzregelungen bei ihrer täglichen Arbeit einhalten?			
Gibt es im Unternehmen Datenschutzschulungen, um Mitarbeiter über ihre Pflichten und die Einhaltung der DSGVO zu informieren?			
Werden die Datenschutzschulungen regelmäßig (mindestens einmal jährlich) wiederholt, um das Bewusstsein und die Kenntnisse der Mitarbeiter aktuell zu halten?			
Werden die Mitarbeiter für das Thema Datenschutz sensibilisiert (z.B. durch geeignete Newsletter oder Workshops)?			

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de

***Hinweise zur Verwendung**

Bei dem vorliegenden Dokument handelt es sich um ein kostenloses Muster, das keinen Anspruch auf Vollständigkeit und Richtigkeit erhebt. Die Vorlage sollte stets auf die individuellen Bedürfnisse und die Umstände des Einzelfalls angepasst und ggf. fachkundig geprüft werden.

Die Vorlage darf für eigene Zwecke oder Zwecke Ihres Unternehmens verwendet werden. Die Weitergabe an Dritte, z.B. an eigene Kunden, sowie die kommerzielle Nutzung sind ohne ausdrückliche Genehmigung nicht gestattet.

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de