Leitlinien für die Anwendung der GDPR in den Sozialsekretariaten

1. Definitionen

1.1. Die in der GDPR verwendeten Definitionen sind in Anhang 1 dargelegt.

1.2. ZSS: Zugelassenes Sozialsekretariat

1.3. GDPR: General Data Protection Regulation. Auf Deutsch abgekürzt „DSGVO“ (Datenschutzgrundverordnung)

1.4. DSB: Datenschutzbehörde, d.h. die Aufsichtsbehörde für den Schutz personenbezogener Daten in Belgien.

1.5. Unterauftragsverarbeiter: der vom Sozialsekretariat ernannte Auftragsverarbeiter, der im Auftrag des Verantwortlichen für einen Teil der Datenverarbeitung des ZSS zuständig ist, darunter u.a. die Verarbeitung personenbezogener Daten.

1.6. USS: Verband der Sozialsekretariate

2. Einleitung

2.1. 90 % der Arbeitgeber im belgischen Privatsektor beauftragen für ihre Sozialverwaltung ein ZSS. Im Rahmen seiner Aufträge verarbeitet das ZSS personenbezogene Daten und ist der Ansicht, dass ein sorgsamer und vertraulicher Umgang mit diesen personenbezogenen Daten äußerst wichtig ist. Zu diesem Zweck sieht der USS die Verwendung von Leitlinien vor, die formelle Angaben für die konkrete Anwendung der GDPR im Sektor der Sozialsekretariate in ihrer Rolle als Auftragsverarbeiter enthalten. Diese Leitlinien geben einen Rahmen vor, innerhalb dessen eine einheitliche Verarbeitung der personenbezogenen Daten der Angestellten der Kunden der Sozialsekretariate sowie die Tatsache, dass diese denselben strengen Schutzmaßnahmen unterliegen, garantiert werden kann.

2.2. Die sektorbezogenen Leitlinien (nachfolgend als „die Leitlinien“ bezeichnet) für die Verarbeitung personenbezogener Daten im Rahmen der GDPR legen auf verständliche Weise die Grundzüge der vom USS umgesetzten Datenschutzstrategie dar.

2.3. Das vorliegende Dokument:

- definiert die Leitlinien für die Verarbeitung personenbezogener Daten im Rahmen der Erbringung von Dienstleistungen;
- verstärkt die Transparenz im Hinblick auf die vom Sektor angewandten Methoden zur Verarbeitung personenbezogener Daten;
- bietet der Datenschutzbehörde („DSB“) Anhaltspunkte für die Überprüfung, ob die Verarbeitung personenbezogener Daten nach den geltenden Gesetzen und Vorschriften erfolgt;

zielt darauf ab, den berechtigten Erwartungen der Kunden hinsichtlich einer korrekten Verarbeitung der personenbezogenen Daten ihrer Mitarbeiter gerecht zu werden.

3. Anwendungsbereich

Die Leitlinien gelten für das in Belgien zugelassene und ansässige Sozialsekretariat und die Ausführung der Hauptaufgaben desselben in Belgien.
Die Leitlinien gelten ausschließlich für die Verarbeitung personenbezogener Daten im Rahmen der Hauptaufgaben des ZSS, und zwar:

- Lohnberechnungen und zugehörige Dokumente
- Angaben gegenüber Behörden und anderen Drittparteien
- Eingang und Entrichtung der LSS-Beträge und des Berufssteuervorabzugs
- rechtliche Beratung in den Bereichen Sozial- und Arbeitsrecht in Bezug auf die Sozialverwaltung des Arbeitgebers

Der Bearbeitungszweck des ZSS in seiner Rolle als Auftragsverarbeiter besteht in der Ausführung der oben genannten Hauptaufgaben.

Im Rahmen der Durchführung dieser Hauptaufgaben verarbeitet das ZSS keine der in Artikel 9 der GDPR aufgeführten besonderen Kategorien personenbezogener Daten.
Vom Kunden/Arbeitgeber bereitgestellte Daten, die nicht für die Ausführung der Hauptaufgaben des ZSS erforderlich sind, fallen nicht in den Anwendungsbereich dieser sektorbezogenen Leitlinien.

4. Beziehung ZSS – Kunde/Arbeitgeber

4.1 Das ZSS ist im Hinblick auf die Ausführung seiner Hauptaufgaben stets Auftragsverarbeiter. Der Verantwortliche ist stets der Kunde/Arbeitgeber.

4.2 Die Rechtsgrundlage für das ZSS ist der Vertrag mit dem Kunden/Arbeitgeber und die für das ZSS als Beauftragtem geltenden gesetzlichen Verpflichtungen.

4. Datenschutz-Folgenabschätzung

Als Auftragsverarbeiter muss das ZSS keine Datenschutz-Folgenabschätzung bzw. Data Protection Impact Assessment (nachfolgend als „AIPD“ bezeichnet) durchführen. Die Verpflichtung zur AIPD liegt de facto ausschließlich beim Verantwortlichen.

Der USS unterstreicht zudem, dass die DSB darauf hinweist, dass es sich bei Lohn- und Personalverwaltung um Verarbeitungstätigkeiten handelt, die keinerlei Verpflichtung zur AIPD unterliegen (Anhang 3 der Empfehlung Nr. 01/2018 vom 28. Februar 2018).

Das ZSS verpflichtet sich gleichwohl zu Folgendem:

- seinen Kunden auf Anfrage dabei zu helfen, ihre Verpflichtungen zur AIPD auf Grundlage des Artikels 35 der GDPR einzuhalten
- eine Analyse der Risiken der für die Kunden durchgeführten Verarbeitungstätigkeiten zu erstellen, damit entsprechende erforderliche technische und organisatorische Maßnahmen ergriffen werden können (vgl. auch Artikel 12 dieser Leitlinien).

4. Verzeichnis von Verarbeitungstätigkeiten

Gemäß Artikel 30.2 der GDPR führt das ZSS ein internes Verzeichnis der Verarbeitungstätigkeiten.

5. Auftragsverarbeiter

Das ZSS, das Unterauftragsverarbeiter für die Durchführung seiner Hauptaufgaben beauftragt,

- schließt mit dem Unterauftragsverarbeiter einen Verarbeitungsvertrag, welcher mindestens dieselben Datenschutzverpflichtungen enthält, wie der jeweilige Verarbeitungsvertrag, den das ZSS mit seinem/seinen Kunden abschließt;
- garantiert, dass der Kunde seine vorherige schriftliche Zustimmung für die Beauftragung von Unterauftragsverarbeitern erteilt. Dies kann in Form einer allgemeinem oder spezifischen schriftlichen Zustimmung geschehen;
- verfügt über eine Arbeitsmethode, die es ermöglicht, jeden Kunden im Voraus über die Hinzunahme oder das Ersetzen eines Unterauftragsverarbeiters zu informieren;
- verfügt über eine Arbeitsmethode zur Bearbeitung der Beschwerde eines Kunden;
- führt eine aktuelle Liste seiner Unterauftragsverarbeiter. Diese Liste steht zumindest auf Nachfrage zur Verfügung.

Das ZSS erachtet die folgenden Drittparteien trotz der Tatsache, dass diese Parteien vom ZSS personenbezogene Daten erhalten, nicht als Unterauftragsverarbeiter:

- die Stellen der sozialen Sicherheit;
- der FÖD Finanzen;
- die Regionalbehörden;
- Organisationen, denen das ZSS auf Anweisung des Kunden personenbezogene Daten der Angestellten des Kunden übermittelt, mit denen das ZSS jedoch keine Vertragsbeziehung hat, zum Beispiel Anbieter von Mahlzeitschecks, Leasing-Firmen, Gruppenversicherungen und Fonds für Existenzsicherheit.

4. Weitergabe personenbezogener Daten an Dritte

Das ZSS gibt Daten ausschließlich im Rahmen seiner Hauptaufgaben oder auf formelle Anweisung des Kunden hin weiter. Diese Anweisungen können vertraglich festgelegt sein oder auf andere Weise erteilt werden (z.B. mithilfe eines Online-Tools).

5. Aufbewahrungsfristen

9.1. Aufbewahrungsfrist für den Kunden/Arbeitgeber als Verantwortlicher in Bezug auf die Aufbewahrung von Dokumenten, für die der Kunde/Arbeitgeber der gesetzlichen Pflicht zur Aufbewahrung unterliegt:

Das ZSS bewahrt die in Anhang 2.1 aufgeführten Dokumente, die es im Rahmen seiner Hauptaufgaben effektiv bearbeitet, mindestens entsprechend der in Anhang 2.1 aufgeführten Aufbewahrungsfrist auf, zu berechnen ab dem Folgejahr nach dem Zeitraum, auf den sich das entsprechende Dokument bezieht, sofern nicht anderweitig mit dem Kunden/Arbeitgeber vereinbart.

9.2. Aufbewahrungsfrist für das ZSS als Auftragsverarbeiter in Bezug auf die Aufbewahrung von Dokumenten, für die das ZSS der gesetzlichen Pflicht zur Aufbewahrung unterliegt:

Das ZSS bewahrt die in Anhang 2.2 aufgeführten Dokumente, die es im Rahmen seiner Hauptaufgaben effektiv bearbeitet, entsprechend der in Anhang 2.2 aufgeführten Aufbewahrungsfrist auf, zu berechnen ab dem Folgejahr nach dem Zeitraum, auf den sich das entsprechende Dokument bezieht.

9.3. Datenspeicherungspolitik

Die Datenspeicherungspolitik des ZSS entspricht dem Grundsatz des Artikels 5.1 der GDPR (Speicherbegrenzung). Die Politik legt mindestens fest, dass das ZSS spätestens 7 Jahre nach Ende des Arbeitsvertrags zwischen dem Kunden und seinem Angestellten und spätestens 7 Jahre nach Ende des Vertrags zwischen dem ZSS und dem Kunden die Löschung/Anonymisierung der Daten veranlasst, sofern nicht anderweitig mit dem Kunden vereinbart.

Die Frist von 7 Jahren beginnt ab dem ersten Tag des Jahres nach Ende des Arbeitsvertrags des Angestellten oder des Vertrags mit dem Kunden. Nach Ablauf der Aufbewahrungsfrist werden die Daten innerhalb einer angemessenen Frist gelöscht oder anonymisiert.

Die Datenspeicherungspolitik berücksichtigt mindestens folgende Elemente:

- ob der Kunde die Möglichkeit hat, die Löschung oder Anonymisierung der personenbezogenen Daten selbst durchzuführen oder nicht;
- wie das ZSS die Aufbewahrung/Löschung/Anonymisierung der personenbezogenen Daten verwaltet;
- die Aufbewahrungsfristen je nach Kategorie der personenbezogenen Daten der Angestellten

9. Datenschutzverantwortlicher

Das ZSS verpflichtet sich, einen Datenschutzverantwortlichen zu ernennen und diese Leitlinien einzuhalten. Dieser Verantwortliche ist ebenfalls die Kontaktperson in Datenschutzfragen. Das ZSS veröffentlicht die Kontaktdaten dieser Person.

Der USS verpflichtet sich, eine Lenkungsgruppe *data protection* („Datenschutz“) einzurichten, die sich aus den Datenschutzverantwortlichen der Mitglieds-Sozialsekretariate des USS zusammensetzt. Aufgaben dieser Lenkungsgruppe sind u.a.:

- Verfolgen der neuen Entwicklungen im Bereich Datenschutz;
- Förderung eines Austauschs bester Praktiken im Sektor;
- Durchführung einer jährlichen Überarbeitung dieser Leitlinien und des Fragebogens zur Selbsteinschätzung.

9. Datenverlust

Sobald das ZSS von einem Datenverlust erfährt, informiert es baldmöglichst den betroffenen Kunden/Arbeitgeber (Verantwortlicher). Das ZSS hat Standardverfahren für die Benachrichtigung des Kunden und den Umgang mit Datenverlust eingerichtet.

Das ZSS leistet dem Verantwortlichen auf Grundlage der verfügbaren Informationen entsprechende Unterstützung im Umgang mit dem Datenverlust.
Der Verantwortliche (Kunde/Arbeitgeber) ist dafür zuständig, zu überprüfen, ob die betroffenen Personen/die Datenschutzbehörde ggf. über den Datenverlust informiert werden müssen. Das ZSS informiert die betroffenen Personen/die Datenschutzbehörde im Falle eines Datenverlusts demnach nicht, sofern nicht anderweitig ausdrücklich mit dem Kunden vereinbart.

10. IT-Sicherheit – technische und organisatorische Maßnahmen

Das ZSS ergreift die für den Schutz der personenbezogenen Daten notwendigen Sicherheitsmaßnahmen wie in Anhang 3 beschrieben. Dieser Anhang bietet einen Überblick über die wichtigsten Maßnahmen, die vom ZSS als Mindestmaßnahmen garantiert werden.

11. Rechte der betroffenen Person

Erhält das ZSS Forderungen der betroffenen Personen zur Ausübung ihrer Rechte, leitet das ZSS diese innerhalb von 14 Kalendertagen an den Kunden/Arbeitgeber weiter.

Das ZSS leistet seinem Kunden/Arbeitgeber angemessene Unterstützung, sodass der Arbeitgeber die Fragen der betroffenen Person sachgerecht beantworten kann.

Das ZSS hat Standardverfahren eingerichtet, die eine Ausübung der Rechte der betroffenen Personen ermöglichen.

12. Einhaltung der Leitlinien

Das ZSS führt mithilfe eines Fragebogens (s. Anhang 4) eine jährliche Selbstbewertung der Anwendung dieser Leitlinien durch und bestätigt dem USS auf Grundlage der Selbstbewertung schriftlich die Einhaltung dieser Leitlinien.

Im Falle von Problemen im Zusammenhang mit einer Nichteinhaltung dieser Leitlinien teilt der USS dies dem betroffenen ZSS mit.

Anhang 1: Definitionen

Diese Leitlinien legen folgende Definitionen zugrunde:

(Definitionen aus der GDPR übernommen)

personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

besondere Kategorien personenbezogener Daten:
personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

- **genetische Daten:** personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;
- **biometrische Daten:** mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;
- **Gesundheitsdaten:** personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

Verarbeitung: jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

betroffene Person: eine identifizierte oder identifizierbare natürliche Person

Verantwortlicher: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das

Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

Auftragsverarbeiter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Dritter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

Datenschutzbeauftragter:
Der Datenschutzbeauftragte überwacht die Datenverarbeitungsvorgänge innerhalb seiner Organisation.

Datenverlust – Verletzung des Schutzes personenbezogener Daten : eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

DPIA (Data Protection Impact Assessment) - Datenschutz-Folgenabschätzung: ein Instrument zur Vorabbewertung von bei der Datenverarbeitung entstehenden Risiken für den Datenschutz natürlicher Personen und zur Durchführung von Maßnahmen zur Reduzierung dieser Risiken. Im Deutschen abgekürzt als DSFA (Datenschutz-Folgenabschätzung).

Anhang 2: Gesetzliche Aufbewahrungsfristen für die im Rahmen der Hauptaufgaben verarbeiteten Daten der Kategorien personenbezogener Daten:

2.1. Gesetzliche Pflichten des Kunden/Arbeitgebers:

Das ZSS gewährt für folgende Dokumente mindestens folgende Aufbewahrungsfristen:

- allgemeine Daten:
  - Stammdaten des Angestellten (Identifikation, Adresse, Bruttolohn, etc.): 5 Jahre
  - Überblick über Löhne und Leistungen: 5 Jahre
  - jeglicher Schriftverkehr zwischen dem Kunden/Arbeitgeber und dem ZSS, der personenbezogene Daten enthält: 5 Jahre

- Lohnberechnungen:
  - die berechneten Daten des Angestellten (detaillierte Lohnberechnung): 5 Jahre
  - Lohnzettel: 5 Jahre
  - individuelle Berechnung: 5 Jahre
  - Buchhaltungsdokumente Löhne: 7 Jahre

- mit der Lohnberechnung zusammenhängende Dokumente:
  - Dienstfahrzeugsbescheinigung: 5 Jahre
  - allgemeines Personalregister: 5 Jahre
  - Dokumente zur Lohnpfändung: 5 Jahre
  - Dokumente zur Lohnabtretung: 5 Jahre
  - Dokumente zur Lohnpfändung wegen Unterhalt: 5 Jahre
  - Dokumente in Bezug auf das Ende eines Arbeitsvertrags (Arbeitsbescheinigung, Urlaubsbescheinigung, ...): 5 Jahre
  - Steuerzettel 281.XX : 7 Jahre
  - Sozialbilanz: 7 Jahre

- Angaben gegenüber Behörden und anderen Drittparteien:
  - DmfA-Quartalsmeldung: 3 Jahre
  - Angaben zu Fonds für Existenzsicherheit: 3 Jahre
  - Dimona-Meldung: 5 Jahre
  - Sozialrisiko-Erklärung Arbeitslosigkeit: 5 Jahre
  - Sozialrisiko-Erklärung Krankheit: 5 Jahre
  - Erklärung zum Berufssteuervorabzug: 7 Jahre

2.2. Spezifische gesetzliche Pflicht des ZSS:

Die Rechtsgrundlage für die spezifischen gesetzlichen Pflichten des ZSS ist in Artikel 48 des KE vom 1. Juli 2006 beschrieben:

Art.48§1. 3°: Das zugelassene Sozialsekretariat ist verpflichtet, für jeden angeschlossenen Arbeitgeber an einem Ort in Belgien ein vollständiges Dossier über die Anwendung der Sozialgesetze für das gesamte Personal des angeschlossenen Arbeitgebers anzulegen und zu führen; dieses Dossier sollte ermöglichen, die Richtigkeit der Angaben zu überprüfen und kann von den in Artikel 31 des Gesetzes genannten Beamten und Bediensteten eingesehen werden; der Inhalt dieses Dossiers wird in den Anweisungen an die Sozialsekretariate bekanntgegeben. (*Übersetzung der französischen Fassung dieses Artikels, Anm. d. Übers.*)

Die konkrete Umsetzung des Artikels 48 des KE vom 1. Juli 2006 ist in den Anweisungen des LSS bezüglich des Arbeitgeber-Dossiers aufgeführt:

Übersicht der im „Einheitlichen Arbeitgeber-Dossier" enthaltenen Elemente:
Zur Ausführung der Bestimmungen von Artikel 48§ 1,3° des KE vom 28.11.1969 sollte das einheitliche Arbeitgeber-Dossier folgende Dokumente oder Informationen in Papierform und/oder elektronischer Form enthalten, und zwar für das gesamte Personal des angeschlossenen Arbeitgebers:

a) den Anschlussvertrag des Arbeitgebers beim ZSS;
b) die dem ZSS erteilte Bevollmächtigung;
c) ein Datenblatt pro Angestelltem mit seinen individuellen Daten (=Auskunftsblatt);
d) die schriftlich und/oder automatisiert festgehaltenen Lohndaten mit Informationen über die von den Angestellten erbrachten Leistungen; derart, dass überprüft werden kann, ob die Auskünfte des Arbeitgebers korrekt in die DmfA-Meldung übertragen worden sind und ob die Sozialabgaben korrekt berechnet worden sind;
e) die Lohnabrechnungen gemäß der Definition im Gesetz über den Lohnschutz (Gesetz vom 12. April 1965);
f) die individuellen Berechnungen aller Angestellten (Identifikationsdaten des Angestellten) gemäß dem KE vom 8. August 1980 über das Anlegen von Sozialdokumenten;
g) jegliche Korrespondenz zwischen dem Arbeitgeber und dem ZSS, die Auswirkungen auf die Pflichten hat oder haben kann, für die das Sozialsekretariat ein Mandat vom Arbeitgeber (auch in elektronischer Form) erhalten hat;
h) ggf., wenn das ZSS beauftragt wurde, die Nettolöhne der Angestellten über das Bankinstitut des Arbeitgebers auszuzahlen, die Dokumente, mit denen dieser Überweisungsauftrag nachgewiesen werden kann;
i) die erhaltenen Urlaubsgeldbescheinigungen, die als Grundlage für die Berechnung des Urlaubsgeldes beim neuen Arbeitgeber gedient haben (wenn nötig, können diese Dokumente mit Festlegung einer Frist angefragt werden);
j) eine Übersicht über die auf den diversen Dokumenten verwendeten Codes mit detaillierten Informationen zu diesen Codes (noch zu konkretisieren);
k) eine Kopie des mit dem/-n betroffenem/-n Arbeitgeber(n) geschlossenen Vertrags oder der Geschäftsordnung des ZSS für seine angeschlossenen Mitglieder.
Konkret bedeutet dies für das ZSS, dass die gesetzlichen Aufbewahrungsfristen für die im Rahmen der Ausführung ihrer Hauptaufgaben verarbeiteten Daten der Kategorien personenbezogener Daten, für welche eine spezifische Aufbewahrungspflicht von 5 Jahren besteht, Folgendes betreffen:

- die Stammdaten des Angestellten (Identifikation, Adresse, Bruttolohn, etc.)

- den Überblick über Löhne und Leistungen
- jeglichen Briefverkehr zwischen dem Kunden/Arbeitgeber und dem ZSS, welcher personenbezogene Daten enthält
- die berechneten Daten des Angestellten (detaillierte Lohnberechnung)
- den Lohnzettel
- die individuelle Berechnung
- Dokumente zum Nachweisen von Überweisungen (wenn das ZSS Nettolöhne auszahlt)
- Dokumente zum Ende eines Arbeitsvertrags (Arbeitsbescheinigung, Urlaubsbescheinigung, ...)

Anhang 3: IT-Sicherheit – technische und organisatorische Maßnahmen

Das ZSS hat die zum Schutz personenbezogener Daten notwendigen Sicherheitsmaßnahmen eingerichtet. Nachfolgend sind die vom ZSS garantierten Mindestmaßnahmen in einem Überblick aufgeführt.

1. **Bereich:**

Sicherheitspolitik und Organisation der IT-Sicherheit

Praktiken:

Zuweisung der Verantwortung für Sicherheit und Datensicherheit. Das ZSS ernennt eine Person, die mitverantwortlich für die Koordination und Kontrolle der Datenschutzregeln und -verfahren ist.

Verantwortlichkeiten. Die Verantwortlichkeiten der Mitarbeiter im Hinblick auf IT-Sicherheit sind definiert und zugewiesen. Das Management schreibt vor, dass alle Mitarbeiter und Auftragnehmer die der geltenden Politik und den Verfahren der Organisation entsprechende IT-Sicherheit anwenden.

2. **Bereich:**

Sichere Personalpolitik

Praktiken:

Vertraulichkeitsverpflichtungen. Die Mitarbeiter des ZSS unterliegen Vertraulichkeitsverpflichtungen und diese Verpflichtungen sind in den Arbeitsverträgen und/oder der Arbeitsordnung formell aufgeführt.

Sensibilisierung. Das ZSS organisiert regelmäßig angemessene Sensibilisierungsaktionen für seine Mitarbeiter.

Beendigung. Die Zugangsrechte werden bei Beendigung der Mitarbeit rechtzeitig entzogen. Dies erfolgt gemäß der Verwaltungsverfahren im Bereich Sicherheit.

3. **Bereich:**

Verwaltung der Betriebsmittel

Praktiken:

Inventar der Betriebsmittel. Das ZSS führt ein aktuelles Inventar jeglichen IT-Materials und der Medien, die es verwendet.

Umgang mit Betriebsmitteln

- Die Regeln für eine annehmbare Verwendung der Informationen und Betriebsmittel sind identifiziert und implementiert.
- Die Angestellten und externe Parteien geben alle in ihrem Besitz befindlichen Betriebsmittel nach der Beendigung des Beschäftigungsverhältnisses oder des Vertrags zurück.

- Das ZSS verfügt über Verfahren zur sicheren Vernichtung von Medien und gedrucktem Material mit vertraulichen Daten.

1. **Bereich:**

Zugangskontrolle

Praktiken:

Zugangsgenehmigung

- Das ZSS sorgt für die Umsetzung und Aufrechterhaltung eines Systems zur Verwaltung der Genehmigungen, welches den Zugang zu Systemen, die Kundendaten enthalten, kontrolliert.
- Jede Person, die Zugang zu Systemen hat, die Kundendaten enthalten, verfügt über eine ID/einen Benutzernamen, die jeweils spezifisch und unverwechselbar sind.
- Das ZSS beschränkt den Zugang zu Kundendaten auf die Personen, welche diesen Zugang zur Ausübung ihrer Funktionen benötigen.

Authentifizierung

- Das ZSS verwendet den Branchenstandards entsprechende Standardpraktiken, um Nutzer, die versuchen, sich Zugang zu den Netzwerk- oder IT-Systemen des ZSS zu verschaffen, zu identifizieren und zu authentifizieren.
- Basieren die Authentifizierungsmechanismen auf dem Gebrauch von Passwörtern, schreibt das ZSS vor, dass das Passwort aus mindestens acht Zeichen bestehen muss.
- Das ZSS gebraucht Praktiken, welche die Vertraulichkeit und Integrität der Passwörter bei der Zuweisung und Vergabe sowie bei der Speicherung derselben garantieren.

Zugang zum Netzwerk. Das ZSS ergreift die notwendigen Kontrollmaßnahmen (z.B. Firewalls, Sicherheitsanwendungen), die im Hinblick auf einen adäquaten Schutz des Zugangs zu seinem Netzwerk ein angemessenes Maß an Sicherheit bieten.

1. **Bereich:**

Kryptografie

Praktiken:

Die Verschlüsselung der vertraulichen Daten erfolgt auf Grundlage der anerkannten Verschlüsselungsstandards (z.B. Transport Layer Security).

2. **Bereich:**

Physische Sicherheit und Sicherung des Umfelds

Praktiken:

Physischer Zugang zu Einrichtungen.

- Das ZSS beschränkt den Zugang zu Einrichtungen, wo vertrauliche Informationen verarbeitet werden, auf die für diese Aufgabe zuständigen Mitarbeiter.
- Der physische Zugang zu den Datenzentren wird nur unter Einhaltung eines formellen Genehmigungsverfahrens gewährt und die Zugangsrechte werden regelmäßig überprüft.

Schutz gegen Störungen. Das ZSS verwendet verschiedene den Branchenstandards entsprechende Systeme zum Schutz seiner Datenzentren gegen Datenverlust infolge von Stromausfall oder im Brandfall.

1. **Bereich:**

Sicherheit der Unternehmensaktivität (Betriebssicherheit)

Praktiken:

Wiederherstellung von Daten

- Das ZSS legt zu Zwecken der Wiederherstellung gemäß der vereinbarten Sicherungskopienpolitik regelmäßig Sicherungskopien der Kundendaten an.
- Das ZSS bewahrt die Kopien der Kundendaten und die Verfahren zur Datenwiederherstellung an einem anderen Ort auf als dem, wo sich der primäre Computer befindet, der die Kundendaten verarbeitet.

Bösartige Software. Das ZSS führt Anti-Malware-Kontrollen durch, um zu verhindern, dass bösartige Software unbefugten Zugang zu Kundendaten erlangt.

Sicherheitsupdate. Sicherheitsupdates werden regelmäßig überprüft und installiert.

Aufzeichnung im Logbuch. Das ZSS führt Buch über den Zugang zu und die Nutzung seiner IT-Systeme, die Kundendaten enthalten, einschließlich Nutzer-ID, Zeitpunkt und betreffende Aktivität.

1. **Bereich:**

Kommunikationssicherheit

Praktiken:

Übertragung außerhalb des eigenen Netzwerks. Das ZSS verschlüsselt die Kundendaten, die über ungesicherte öffentliche Netzwerke übertragen werden.

Informationsweitergabe. Die Weitergabe von Kundendaten an Dritte erfolgt ausschließlich auf Anweisung des Kunden.

2. **Bereich:**

Erwerb, Entwicklung und Wartung der IT-Systeme

Praktiken:

Sicherheitsanforderungen. Für jegliche Entwicklung werden die Datenschutzanforderungen von Beginn an analysiert und umgesetzt (security und privacy by design).

Trennung von Entwicklung und Produktion. Die Zugangsrechte für die Produktion sind auf die Mitarbeiter der Sozialsekretariate beschränkt, welche den Zugang zum Produktionsbereich im Rahmen ihrer Funktion benötigen.

Kontrolle von Veränderungen. Das ZSS (oder sein IT-Dienstanbieter) hat ein Änderungskontrollverfahren eingerichtet, um sicherzustellen, dass Änderungen an den Betriebssystemen und operativen Anwendungen kontrolliert erfolgen.

3. **Bereich:**

Beziehungen zu Dienstanbietern

Praktiken:

Auswahl der Dienstanbieter. Das ZSS wendet ein Auswahlverfahren an, bei welchem die Sicherheits- und Datenschutzpraktiken eines Dienstanbieters/Partners bei der Datenverarbeitung bewertet werden.

Vertragspflichten. Die Dienstanbieter mit Zugang zu Kundendaten unterliegen Datenschutzverpflichtungen, welche formell in den Verträgen mit den Dienstanbietern aufgeführt sind.

4. **Bereich:**

Umgang mit IT-sicherheitsbezogenen Vorfällen

Praktiken:

Meldung der Vorfälle. Bei einem IT-sicherheitsbezogenen Vorfall, welcher Auswirkungen auf die Vertraulichkeit oder Integrität der Kundendaten hat, informiert das ZSS den Kunden ohne unangemessene Verzögerung.

5. **Bereich:**

Betriebskontinuität

Praktiken:

Notfallwiederherstellung. Das ZSS garantiert das Bestehen eines Notfallplans zur Wiederherstellung für die Datenzentren, wo sich die IT-Systeme des ZSS befinden, die Kundendaten verarbeiten.

Redundanz. Das ZSS verfügt über redundante Datenspeicher und Verfahren zur Datenwiederherstellung. Diese werden zu dem Zweck erstellt, Kundendaten in dem Zustand wiederherzustellen zu können, in dem sie zuletzt vor einem Verlust oder der Vernichtung von Daten gespeichert worden sind.

6. **Bereich:**

Einhaltung

Praktiken:

Sicherheitsbewertung. Die Einhaltung der IT-Sicherheitskontrollen wird regelmäßig überprüft.

Anhang 4: Fragebogen zur jährlichen Bewertung der Einhaltung der Leitlinien
Siehe WORD-Dokument