Datenschutzreglement der Yushin-Ryu AG

Kapitel 1 – Allgemeine Bestimmungen

Art. 1 Zweck

Dieses Datenschutzreglement regelt die Grundsätze, Verantwortlichkeiten sowie organisatorischen und technischen Maßnahmen zum Schutz personenbezogener Daten innerhalb der Yushin-Ryu AG.

Es dient der rechtskonformen Verarbeitung personenbezogener Daten sowie dem Schutz der Persönlichkeitsrechte von natürlichen Personen.

Art. 2 Zielsetzung

Dieses Reglement verfolgt insbesondere folgende Ziele:

- Schutz personenbezogener Daten;
- Einhaltung der gesetzlichen Datenschutzvorschriften;
- Sicherstellung der Vertraulichkeit;
- Sicherstellung der Integrität;
- Sicherstellung der Verfügbarkeit;
- Förderung eines verantwortungsvollen Umgangs mit personenbezogenen Daten;
- Unterstützung der Corporate Governance.

Art. 3 Geltungsbereich

Dieses Reglement gilt für:

- den Verwaltungsrat;
- den Präsidenten des Verwaltungsrates;
- den Chief Visionary Officer (CVO);
- den Chief Executive Officer (CEO);
- sämtliche Mitglieder der Geschäftsleitung;
- alle Mitarbeitenden;
- alle Fakultäten;
- alle Institute;
- alle Fachbereiche;
- alle Studierenden;
- alle externen Auftragnehmenden, soweit vertraglich vereinbart;

- sämtliche Tochtergesellschaften und Standorte der Yushin-Ryu AG, soweit anwendbar.

Art. 4 Grundsatz

Personenbezogene Daten dürfen ausschließlich nach den geltenden gesetzlichen Vorschriften sowie nach den Bestimmungen dieses Reglements verarbeitet werden.

Jede Verarbeitung hat rechtmäßig, transparent, zweckgebunden und verhältnismäßig zu erfolgen.

Art. 5 Begriffsbestimmungen

Im Sinne dieses Reglements gelten insbesondere folgende Begriffe:

- personenbezogene Daten;
- besonders schützenswerte Personendaten;
- Bearbeitung bzw. Verarbeitung;
- betroffene Person;
- Verantwortlicher;
- Auftragsbearbeiter;
- Einwilligung;
- Datenschutzverletzung.

Die jeweils geltenden gesetzlichen Definitionen sind maßgebend.

Art. 6 Rechtsgrundlagen

Die Yushin-Ryu AG richtet ihr Datenschutzmanagement insbesondere nach den jeweils anwendbaren gesetzlichen Datenschutzbestimmungen der Staaten aus, in denen sie tätig ist.

Hierzu gehören insbesondere die datenschutzrechtlichen Anforderungen der Schweiz sowie weiterer Staaten und Regionen, soweit diese auf die Tätigkeit der Gesellschaft Anwendung finden.

Art. 7 Datenschutzgrundsätze

Bei jeder Verarbeitung personenbezogener Daten sind insbesondere folgende Grundsätze einzuhalten:

- Rechtmäßigkeit;
- Treu und Glauben;
- Transparenz;
- Zweckbindung;
- Datenminimierung;
- Richtigkeit;
- Speicherbegrenzung;
- Integrität;
- Vertraulichkeit;
- Rechenschaftspflicht.

Art. 8 Datenschutzorganisation

Die Yushin-Ryu AG richtet eine angemessene Datenschutzorganisation ein.

Die Verantwortlichkeiten sind eindeutig festzulegen und regelmäßig zu überprüfen.

Art. 9 Verantwortung

Die Gesamtverantwortung für den Datenschutz trägt der Verwaltungsrat.

Die strategische Steuerung erfolgt durch den CEO und den CVO.

Die operative Koordination obliegt der hierfür bestimmten Datenschutzfunktion bzw. dem Datenschutzbeauftragten.

Alle Führungskräfte tragen Verantwortung für die Einhaltung des Datenschutzes innerhalb ihres jeweiligen Zuständigkeitsbereiches.

Art. 10 Zusammenarbeit

Der Datenschutz arbeitet insbesondere zusammen mit:

- Informationssicherheit;
- Qualitätsmanagement;
- Compliance;
- Risikomanagement;
- Personal;
- IT;
- Forschung;
- Lehre;
- Rechtsabteilung;
- Interner Revision.

Kapitel 2 – Datenschutzgrundsätze

Art. 11 Grundsatz

Die Verarbeitung personenbezogener Daten erfolgt nach den Grundsätzen der Rechtmäßigkeit, Fairness, Transparenz, Zweckbindung und Verhältnismäßigkeit.

Jede Verarbeitung ist auf das notwendige Maß zu beschränken.

Art. 12 Rechtmäßigkeit

Personenbezogene Daten dürfen ausschließlich auf einer gesetzlichen Grundlage, einer vertraglichen Grundlage, einer Einwilligung oder einem sonstigen zulässigen Rechtfertigungsgrund verarbeitet werden.

Art. 13 Zweckbindung

Personenbezogene Daten dürfen ausschließlich für die festgelegten, eindeutigen und rechtmäßigen Zwecke verarbeitet werden.

Eine Weiterverarbeitung für unvereinbare Zwecke ist unzulässig.

Art. 14 Datenminimierung

Es dürfen ausschließlich diejenigen personenbezogenen Daten erhoben und verarbeitet werden, die für den jeweiligen Zweck erforderlich sind.

Nicht erforderliche Daten sind weder zu erheben noch dauerhaft zu speichern.

Art. 15 Richtigkeit

Personenbezogene Daten müssen sachlich richtig und, soweit erforderlich, aktuell sein.

Unrichtige oder unvollständige Daten sind unverzüglich zu berichtigen oder zu löschen.

Art. 16 Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für den jeweiligen Verarbeitungszweck oder aufgrund gesetzlicher Aufbewahrungspflichten erforderlich ist.

Nach Ablauf der Aufbewahrungsfrist sind die Daten zu löschen oder zu anonymisieren, sofern keine gesetzlichen Gründe entgegenstehen.

Art. 17 Integrität und Vertraulichkeit

Personenbezogene Daten sind durch geeignete technische und organisatorische Maßnahmen gegen:

- unbefugten Zugriff;
- Verlust;
- Manipulation;
- Zerstörung;
- unbefugte Offenlegung;
- Missbrauch

zu schützen.

Art. 18 Rechenschaftspflicht

Die Yushin-Ryu AG weist die Einhaltung der Datenschutzvorschriften durch geeignete Dokumentationen, Nachweise und Kontrollen nach.

Art. 19 Datenschutz durch Technikgestaltung

Neue Prozesse, Systeme und Anwendungen sind bereits bei ihrer Planung datenschutzgerecht auszugestalten.

Datenschutzanforderungen sind frühzeitig in Projekte zu integrieren.

Art. 20 Datenschutz durch datenschutzfreundliche Voreinstellungen

Systeme und Anwendungen sind grundsätzlich so zu konfigurieren, dass nur diejenigen personenbezogenen Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind.

Standardmäßig sind datenschutzfreundliche Einstellungen zu verwenden.

Kapitel 3 – Rechte der betroffenen Personen

Art. 21 Grundsatz

Die Yushin-Ryu AG gewährleistet die gesetzlich vorgesehenen Rechte der betroffenen Personen.

Entsprechende Anfragen sind sorgfältig, fristgerecht und nachvollziehbar zu bearbeiten.

Art. 22 Informationsrecht

Betroffene Personen sind in geeigneter Weise über die Verarbeitung ihrer personenbezogenen Daten zu informieren.

Die Information umfasst insbesondere:

- Zweck der Datenverarbeitung;
- Rechtsgrundlage;
- Kategorien der bearbeiteten Daten;
- Empfänger oder Kategorien von Empfängern;
- Speicherdauer;
- Rechte der betroffenen Person;
- Kontaktstelle für Datenschutzanfragen.

Art. 23 Auskunftsrecht

Jede betroffene Person hat das Recht, Auskunft darüber zu verlangen, ob personenbezogene Daten über sie verarbeitet werden.

Die Auskunft umfasst insbesondere:

- die verarbeiteten Daten;
- den Verarbeitungszweck;
- die Herkunft der Daten, soweit bekannt;
- Empfänger der Daten;
- Speicherdauer;
- gesetzliche Grundlagen.

Art. 24 Recht auf Berichtigung

Unrichtige oder unvollständige personenbezogene Daten sind auf Antrag oder von Amtes wegen unverzüglich zu berichtigen oder zu vervollständigen.

Art. 25 Recht auf Löschung

Personenbezogene Daten sind zu löschen, sofern:

- der Verarbeitungszweck weggefallen ist;
- keine gesetzliche Aufbewahrungspflicht besteht;
- eine Einwilligung wirksam widerrufen wurde;
- die Verarbeitung unzulässig ist;
- gesetzliche Löschpflichten bestehen.

Art. 26 Recht auf Einschränkung der Verarbeitung

Die Verarbeitung personenbezogener Daten ist einzuschränken, soweit dies gesetzlich vorgesehen ist oder berechtigte Interessen der betroffenen Person dies erfordern.

Art. 27 Recht auf Datenübertragbarkeit

Soweit gesetzlich vorgesehen, können betroffene Personen verlangen, ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder an einen anderen Verantwortlichen übertragen zu lassen.

Art. 28 Widerspruchsrecht

Betroffene Personen können der Verarbeitung ihrer personenbezogenen Daten widersprechen, sofern hierfür gesetzliche Voraussetzungen bestehen.

Der Widerspruch ist sorgfältig zu prüfen und entsprechend den gesetzlichen Vorgaben zu behandeln.

Art. 29 Widerruf einer Einwilligung

Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Der Widerruf berührt nicht die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung.

Art. 30 Bearbeitung von Anträgen

Anträge betroffener Personen sind unverzüglich an die zuständige Datenschutzfunktion weiterzuleiten.

Die Bearbeitung erfolgt fristgerecht, nachvollziehbar und unter Beachtung der gesetzlichen Anforderungen.

Datenschutzreglement der Yushin-Ryu AG

Kapitel 4 – Verantwortlichkeiten und Datenschutzorganisation

Art. 31 Grundsatz

Die Yushin-Ryu AG richtet eine klare Datenschutzorganisation mit eindeutig geregelten Verantwortlichkeiten, Kompetenzen und Berichtslinien ein.

Der Datenschutz ist Bestandteil der Corporate Governance sowie des integrierten Managementsystems der Gesellschaft.

Art. 32 Verwaltungsrat

Der Verwaltungsrat trägt die oberste Verantwortung für den Datenschutz innerhalb der Yushin-Ryu AG.

Er genehmigt insbesondere:

- die Datenschutzstrategie;
- dieses Datenschutzreglement;
- wesentliche Datenschutzrichtlinien;
- grundlegende organisatorische Maßnahmen.

Art. 33 Chief Visionary Officer (CVO)

Der CVO stellt sicher, dass der Datenschutz langfristig in die strategische Entwicklung der Gesellschaft sowie in nationale und internationale Projekte integriert wird.

Art. 34 Chief Executive Officer (CEO)

Der CEO trägt die Gesamtverantwortung für die operative Umsetzung der Datenschutzstrategie.

Er stellt die erforderlichen personellen, organisatorischen und finanziellen Ressourcen zur Verfügung.

Art. 35 Datenschutzbeauftragter

Die Gesellschaft bestimmt eine für den Datenschutz verantwortliche Funktion.

Diese ist insbesondere zuständig für:

- Beratung der Organisationseinheiten;
- Unterstützung der Geschäftsleitung;
- Überwachung der Einhaltung dieses Reglements;
- Koordination datenschutzrelevanter Fragestellungen;
- Unterstützung bei Datenschutzvorfällen.

Art. 36 Führungskräfte

Alle Führungskräfte tragen Verantwortung für den Datenschutz innerhalb ihres jeweiligen Zuständigkeitsbereiches.

Sie haben insbesondere:

- datenschutzkonforme Prozesse sicherzustellen;
- Mitarbeitende zu sensibilisieren;
- Datenschutzverstöße unverzüglich zu melden;
- Datenschutzmaßnahmen umzusetzen.

Art. 37 Mitarbeitende

Alle Mitarbeitenden sind verpflichtet,

- personenbezogene Daten vertraulich zu behandeln;
- dieses Reglement einzuhalten;
- Datenschutzverstöße unverzüglich zu melden;
- an Datenschutzschulungen teilzunehmen;
- personenbezogene Daten ausschließlich im Rahmen ihrer Aufgaben zu bearbeiten.

Art. 38 Zusammenarbeit

Der Datenschutz arbeitet insbesondere zusammen mit:

- Qualitätsmanagement;
- Compliance;
- Risikomanagement;
- Informationssicherheit;
- Personal;
- IT;
- Rechtsdienst;
- Interner Revision;
- Forschung;
- Lehre.

Art. 39 Datenschutz in Projekten

Bereits bei der Planung neuer Projekte, Systeme, Prozesse oder Organisationsänderungen sind die datenschutzrechtlichen Anforderungen angemessen zu berücksichtigen.

Art. 40 Berichtswesen

Die Datenschutzfunktion berichtet regelmäßig an die Geschäftsleitung über:

- den Stand des Datenschutzmanagements;
- wesentliche Datenschutzvorfälle;
- Risiken;
- Verbesserungsmaßnahmen;
- Schulungsstand;
- Ergebnisse interner Überprüfungen.

Kapitel 5 – Verarbeitung personenbezogener Daten

Art. 41 Grundsatz

Personenbezogene Daten dürfen ausschließlich für festgelegte, eindeutige und rechtmäßige Zwecke bearbeitet werden.

Jede Bearbeitung hat nach den Grundsätzen dieses Reglements sowie den anwendbaren gesetzlichen Datenschutzvorschriften zu erfolgen.

Art. 42 Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist zulässig, sofern hierfür eine gesetzliche Grundlage, eine vertragliche Grundlage, eine wirksame Einwilligung oder ein anderer anerkannter Rechtfertigungsgrund besteht.

Art. 43 Zweckbindung

Personenbezogene Daten dürfen ausschließlich zu dem Zweck verwendet werden, für den sie erhoben wurden.

Eine Änderung des Verarbeitungszwecks ist nur zulässig, sofern hierfür eine rechtliche Grundlage besteht.

Art. 44 Datenminimierung

Es dürfen ausschließlich diejenigen personenbezogenen Daten erhoben, verarbeitet und gespeichert werden, welche zur Erfüllung des jeweiligen Zwecks erforderlich sind.

Art. 45 Richtigkeit der Daten

Die verantwortlichen Organisationseinheiten stellen sicher, dass personenbezogene Daten sachlich richtig, vollständig und aktuell sind.

Unrichtige Daten sind unverzüglich zu berichtigen oder zu löschen.

Art. 46 Speicherung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies:

- zur Erfüllung des jeweiligen Zweckes,
- aufgrund gesetzlicher Aufbewahrungspflichten,
- aufgrund vertraglicher Verpflichtungen oder
- aufgrund berechtigter Interessen

erforderlich ist.

Art. 47 Löschung und Anonymisierung

Nach Wegfall des Verarbeitungszwecks sind personenbezogene Daten entsprechend den gesetzlichen Vorgaben zu löschen oder, soweit möglich und zweckmäßig, zu anonymisieren.

Art. 48 Besondere Kategorien personenbezogener Daten

Besonders schützenswerte personenbezogene Daten unterliegen erhöhten organisatorischen und technischen Schutzmaßnahmen.

Ihre Verarbeitung bedarf besonderer Sorgfalt sowie einer entsprechenden rechtlichen Grundlage.

Art. 49 Verarbeitung im Beschäftigungsverhältnis

Personenbezogene Daten von Mitarbeitenden dürfen ausschließlich verarbeitet werden, soweit dies für:

- das Arbeitsverhältnis,
- gesetzliche Verpflichtungen,
- Sozialversicherungen,
- Lohnabrechnung,
- Personalentwicklung,
- Arbeitssicherheit oder
- berechtigte betriebliche Interessen

erforderlich ist.

Art. 50 Verarbeitung im Studienbetrieb

Personenbezogene Daten von Studierenden dürfen insbesondere verarbeitet werden für:

- Zulassungsverfahren;

- Immatrikulation;
- Studienorganisation;
- Prüfungswesen;
- Leistungsnachweise;
- Studienberatung;
- Alumni-Verwaltung;
- gesetzliche Meldepflichten.

Kapitel 6 – Datenweitergabe und Auftragsbearbeitung

Art. 51 Grundsatz

Die Weitergabe personenbezogener Daten erfolgt ausschließlich im Rahmen der geltenden gesetzlichen Bestimmungen sowie der Bestimmungen dieses Reglements.

Eine Weitergabe hat nach den Grundsätzen der Vertraulichkeit, Zweckbindung und Datenminimierung zu erfolgen.

Art. 52 Interne Datenweitergabe

Innerhalb der Yushin-Ryu AG dürfen personenbezogene Daten ausschließlich an diejenigen Organisationseinheiten weitergegeben werden, welche diese zur Erfüllung ihrer gesetzlichen, vertraglichen oder dienstlichen Aufgaben benötigen.

Art. 53 Externe Datenweitergabe

Eine Weitergabe personenbezogener Daten an externe Stellen ist ausschließlich zulässig, sofern:

- eine gesetzliche Verpflichtung besteht;
- eine vertragliche Grundlage vorliegt;
- eine wirksame Einwilligung erteilt wurde;
- ein sonstiger gesetzlich zulässiger Rechtfertigungsgrund besteht.

Art. 54 Auftragsbearbeitung

Werden personenbezogene Daten durch externe Dienstleister verarbeitet, ist eine den gesetzlichen Anforderungen entsprechende Vereinbarung zur Auftragsbearbeitung abzuschließen.

Die Gesellschaft bleibt für die Auswahl und Überwachung der Auftragsbearbeiter verantwortlich.

Art. 55 Auswahl von Auftragsbearbeitern

Auftragsbearbeiter sind sorgfältig auszuwählen.

Dabei sind insbesondere zu prüfen:

- Fachkompetenz;
- Datenschutzorganisation;
- Informationssicherheit;
- technische und organisatorische Maßnahmen;
- Zuverlässigkeit;
- gesetzliche Konformität.

Art. 56 Kontrolle von Auftragsbearbeitern

Die Gesellschaft überprüft regelmäßig, ob Auftragsbearbeiter die vereinbarten Datenschutzanforderungen einhalten.

Festgestellte Mängel sind unverzüglich zu beheben.

Art. 57 Gemeinsame Verantwortlichkeit

Werden personenbezogene Daten gemeinsam mit anderen Organisationen verarbeitet, sind die jeweiligen Verantwortlichkeiten eindeutig festzulegen und schriftlich zu dokumentieren.

Art. 58 Internationale Datenübermittlungen

Werden personenbezogene Daten in andere Staaten übermittelt oder von dort aus verarbeitet, sind die jeweils anwendbaren gesetzlichen Anforderungen sowie die internen Datenschutzstandards der Yushin-Ryu AG einzuhalten.

Erforderliche Schutzmaßnahmen sind vor der Datenübermittlung umzusetzen.

Art. 59 Vertraulichkeit

Alle Personen, die Zugang zu personenbezogenen Daten erhalten, sind zur Vertraulichkeit verpflichtet.

Diese Verpflichtung besteht auch nach Beendigung des Arbeits-, Dienstleistungs- oder Vertragsverhältnisses fort.

Art. 60 Dokumentation

Sämtliche wesentlichen Datenweitergaben sowie Auftragsbearbeitungen sind vollständig, nachvollziehbar und revisionssicher zu dokumentieren.

Kapitel 7 – Technische und organisatorische Datenschutzmaßnahmen (TOM)

Art. 61 Grundsatz

Die Yushin-Ryu AG trifft angemessene technische und organisatorische Maßnahmen (TOM), um personenbezogene Daten vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor Verlust, Zerstörung, Veränderung oder unbefugter Offenlegung zu schützen.

Die Maßnahmen sind regelmäßig auf ihre Wirksamkeit zu überprüfen und bei Bedarf anzupassen.

Art. 62 Zielsetzung

Die technischen und organisatorischen Maßnahmen dienen insbesondere:

- der Sicherstellung der Vertraulichkeit;
- der Sicherstellung der Integrität;
- der Sicherstellung der Verfügbarkeit;
- der Sicherstellung der Authentizität;
- der Sicherstellung der Nachvollziehbarkeit;
- der Gewährleistung eines angemessenen Datenschutzniveaus.

Art. 63 Zutrittskontrolle

Gebäude, Serverräume, Archive sowie sonstige Bereiche mit personenbezogenen Daten sind gegen unbefugten Zutritt zu schützen.

Hierzu können insbesondere eingesetzt werden:

- Schließsysteme;
- elektronische Zutrittskontrollen;
- Besuchermanagement;
- Videoüberwachung, soweit gesetzlich zulässig.

Art. 64 Zugangskontrolle

Der Zugang zu informationsverarbeitenden Systemen erfolgt ausschließlich für autorisierte Personen.

Hierzu sind insbesondere geeignete Authentifizierungsverfahren einzusetzen.

Art. 65 Zugriffskontrolle

Personenbezogene Daten dürfen ausschließlich von Personen eingesehen oder bearbeitet werden, welche hierzu aufgrund ihrer Funktion berechtigt sind.

Die Zugriffsrechte sind regelmäßig zu überprüfen.

Art. 66 Weitergabekontrolle

Die Übermittlung personenbezogener Daten ist durch geeignete organisatorische und technische Maßnahmen gegen unbefugte Offenlegung zu schützen.

Art. 67 Eingabekontrolle

Die Verarbeitung personenbezogener Daten soll nachvollziehbar dokumentiert werden.

Soweit technisch möglich und erforderlich, sind Änderungen, Eingaben und Löschungen protokolliert.

Art. 68 Verfügbarkeitskontrolle

Die Verfügbarkeit personenbezogener Daten ist durch geeignete Maßnahmen sicherzustellen.

Hierzu gehören insbesondere:

- Datensicherungen;
- Backup-Konzepte;
- Notfallplanung;
- Wiederherstellungsverfahren;
- Redundanzen kritischer Systeme.

Art. 69 Trennungsgebot

Personenbezogene Daten, die für unterschiedliche Zwecke verarbeitet werden, sind organisatorisch oder technisch voneinander zu trennen, soweit dies erforderlich ist.

Art. 70 Regelmäßige Überprüfung

Die technischen und organisatorischen Maßnahmen sind regelmäßig auf ihre Aktualität, Angemessenheit und Wirksamkeit zu überprüfen.

Festgestellte Schwachstellen sind zeitnah zu beheben.

Kapitel 8 – Datenschutzverletzungen und Meldeverfahren

Art. 71 Grundsatz

Datenschutzverletzungen sind unverzüglich zu erkennen, zu melden, zu dokumentieren und angemessen zu behandeln.

Ziel ist es, Schäden für betroffene Personen sowie für die Yushin-Ryu AG möglichst zu verhindern oder zu begrenzen.

Art. 72 Datenschutzverletzung

Als Datenschutzverletzung gilt insbesondere jede Verletzung der Sicherheit, welche zur unbeabsichtigten oder unrechtmäßigen:

- Vernichtung;
- Veränderung;
- Offenlegung;
- Verlust;
- unbefugten Verarbeitung;
- unbefugten Übermittlung;
- unbefugten Zugänglichmachung

personenbezogener Daten führt.

Art. 73 Meldepflicht

Alle Mitarbeitenden sind verpflichtet, vermutete oder festgestellte Datenschutzverletzungen unverzüglich der zuständigen Datenschutzfunktion oder der hierfür bestimmten Meldestelle zu melden.

Art. 74 Sofortmaßnahmen

Nach Eingang einer Meldung sind unverzüglich geeignete Sofortmaßnahmen einzuleiten.

Diese umfassen insbesondere:

- Sicherung von Beweismitteln;
- Begrenzung des Schadens;
- Wiederherstellung betroffener Systeme;
- Schutz weiterer personenbezogener Daten;
- Information der zuständigen Stellen.

Art. 75 Untersuchung

Jede Datenschutzverletzung ist systematisch zu untersuchen.

Hierbei sind insbesondere festzustellen:

- Ursache;
- Umfang;
- betroffene Daten;
- betroffene Personen;
- mögliche Auswirkungen;
- erforderliche Folgemaßnahmen.

Art. 76 Risikobewertung

Jede Datenschutzverletzung ist hinsichtlich ihres Risikos für die betroffenen Personen zu bewerten.

Die Bewertung erfolgt unter Berücksichtigung von:

- Art der Daten;
- Umfang der Daten;
- Anzahl der betroffenen Personen;
- Eintrittswahrscheinlichkeit möglicher Schäden;
- Schwere möglicher Auswirkungen.

Art. 77 Meldepflicht gegenüber Behörden

Soweit gesetzlich vorgeschrieben, sind Datenschutzverletzungen fristgerecht den zuständigen Aufsichts- oder Datenschutzbehörden zu melden.

Die Verantwortung hierfür trägt die zuständige Datenschutzfunktion in Abstimmung mit der Geschäftsleitung.

Art. 78 Information betroffener Personen

Sind betroffene Personen voraussichtlich erheblichen Risiken ausgesetzt, sind diese entsprechend den gesetzlichen Anforderungen in geeigneter Weise zu informieren.

Die Information erfolgt sachlich, nachvollziehbar und möglichst zeitnah.

Art. 79 Dokumentation

Sämtliche Datenschutzverletzungen sind vollständig und revisionssicher zu dokumentieren.

Die Dokumentation umfasst insbesondere:

- Zeitpunkt des Vorfalls;
- Beschreibung;
- Ursache;
- Auswirkungen;
- eingeleitete Maßnahmen;
- Meldungen an Behörden;

- Information betroffener Personen;
- Abschlussbewertung.

Art. 80 Lessons Learned

Nach Abschluss der Bearbeitung sind Datenschutzverletzungen auszuwerten.

Erkenntnisse fließen in:

- das Datenschutzmanagement;
- das Informationssicherheitsmanagement;
- das Risikomanagement;
- das Qualitätsmanagement;
- Schulungsmaßnahmen;
- technische und organisatorische Verbesserungen

ein.

Kapitel 9 – Datenschutz-Folgenabschätzung und Datenschutzprüfung

Art. 81 Grundsatz

Vor Verarbeitungsvorgängen mit erhöhtem Risiko für die Rechte und Freiheiten betroffener Personen ist eine Datenschutz-Folgenabschätzung (DSFA) oder eine gleichwertige datenschutzrechtliche Prüfung durchzuführen.

Die Prüfung erfolgt vor Aufnahme der Datenverarbeitung.

Art. 82 Zielsetzung

Die Datenschutz-Folgenabschätzung dient insbesondere:

- der frühzeitigen Erkennung datenschutzrechtlicher Risiken;
- der Bewertung möglicher Auswirkungen auf betroffene Personen;
- der Festlegung geeigneter Schutzmaßnahmen;
- der Sicherstellung rechtskonformer Datenverarbeitungen;
- der Unterstützung einer risikoorientierten Unternehmensführung.

Art. 83 Anwendungsfälle

Eine Datenschutz-Folgenabschätzung ist insbesondere zu prüfen bei:

- Einführung neuer IT-Systeme;
- Einführung neuer digitaler Dienstleistungen;
- Forschungsprojekten mit personenbezogenen Daten;
- Verarbeitung besonders schützenswerter Personendaten;
- umfangreicher automatisierter Datenverarbeitung;
- Einsatz neuer Technologien;
- internationalen Datenübermittlungen mit erhöhtem Risiko.

Art. 84 Durchführung

Die Datenschutz-Folgenabschätzung umfasst mindestens:

- Beschreibung der geplanten Verarbeitung;
- Zweck der Verarbeitung;
- Bewertung der Erforderlichkeit;
- Bewertung der Verhältnismäßigkeit;
- Risikoanalyse;
- geplante Schutzmaßnahmen;
- Restrisikobewertung.

Art. 85 Beteiligte Stellen

Die Datenschutz-Folgenabschätzung erfolgt unter Einbezug der zuständigen Organisationseinheiten.

Hierzu gehören insbesondere:

- Datenschutzfunktion;
- Informationssicherheit;
- Qualitätsmanagement;
- Risikomanagement;
- IT;
- Rechtsdienst;
- verantwortliche Fachbereiche.

Art. 86 Genehmigung

Verarbeitungsvorgänge mit erhöhtem Datenschutzrisiko dürfen erst nach Abschluss der Datenschutzprüfung sowie nach Freigabe durch die zuständige Stelle aufgenommen werden.

Art. 87 Dokumentation

Datenschutz-Folgenabschätzungen sind vollständig, nachvollziehbar und revisionssicher zu dokumentieren.

Die Dokumentation ist entsprechend den internen Aufbewahrungsfristen zu archivieren.

Art. 88 Überprüfung

Datenschutz-Folgenabschätzungen sind regelmäßig sowie bei wesentlichen Änderungen der Verarbeitung zu überprüfen und erforderlichenfalls zu aktualisieren.

Art. 89 Beratung

Die Datenschutzfunktion unterstützt die Organisationseinheiten bei der Durchführung datenschutzrechtlicher Prüfungen sowie bei der Bewertung datenschutzrechtlicher Risiken.

Art. 90 Kontinuierliche Verbesserung

Erkenntnisse aus Datenschutz-Folgenabschätzungen sind systematisch auszuwerten.

Geeignete Verbesserungsmaßnahmen sind in Prozesse, Systeme und organisatorische Regelungen zu übernehmen.

Kapitel 10 – Schulung, Sensibilisierung und Datenschutzkultur

Art. 91 Grundsatz

Die Yushin-Ryu AG fördert eine nachhaltige Datenschutzkultur durch regelmäßige Schulungen, Sensibilisierungsmaßnahmen sowie den kontinuierlichen Ausbau der Datenschutzkompetenz aller Organe, Führungskräfte und Mitarbeitenden.

Art. 92 Zielsetzung

Die Schulungs- und Sensibilisierungsmaßnahmen dienen insbesondere:

- der Förderung des Datenschutzbewusstseins;
- der rechtskonformen Verarbeitung personenbezogener Daten;
- der Erkennung datenschutzrechtlicher Risiken;
- der Vermeidung von Datenschutzverletzungen;
- der kontinuierlichen Verbesserung des Datenschutzmanagementsystems.

Art. 93 Pflichtschulungen

Pflichtschulungen sind insbesondere durchzuführen für:

- Mitglieder des Verwaltungsrates;
- Geschäftsleitung;
- C-Level-Führungskräfte;
- Führungskräfte;
- Mitarbeitende mit Zugriff auf personenbezogene Daten;
- Personalabteilung;
- IT;
- Forschung;
- Studierendenverwaltung;
- weitere datenschutzrelevante Organisationseinheiten.

Art. 94 Schulungsinhalte

Die Schulungen umfassen insbesondere:

- Datenschutzgrundsätze;
- Rechte betroffener Personen;
- gesetzliche Anforderungen;
- Informationssicherheit;
- technische und organisatorische Maßnahmen;
- Datenschutzverletzungen;
- Meldeverfahren;
- Aufbewahrungs- und Löschfristen;
- sichere Datenverarbeitung.

Art. 95 Spezialschulungen

Für Organisationseinheiten mit erhöhtem Datenschutzrisiko sind ergänzende Spezialschulungen durchzuführen.

Dies betrifft insbesondere:

- Forschung;
- Medizin;
- Personalwesen;
- IT;
- internationale Kooperationen;
- Cloud-Dienste;
- künstliche Intelligenz;
- Laborbereiche.

Art. 96 Sensibilisierung

Die Gesellschaft führt regelmäßig Maßnahmen zur Sensibilisierung für Datenschutz und Informationssicherheit durch.

Hierzu können insbesondere gehören:

- Informationsveranstaltungen;
- Merkblätter;
- E-Learning-Angebote;
- Workshops;
- Praxisübungen;
- interne Informationskampagnen.

Art. 97 Datenschutzkultur

Alle Organe, Führungskräfte und Mitarbeitenden tragen Verantwortung für einen verantwortungsvollen Umgang mit personenbezogenen Daten.

Datenschutz ist Bestandteil der Unternehmenskultur und der täglichen Arbeitsabläufe.

Art. 98 Wissensmanagement

Datenschutzrelevantes Wissen ist systematisch zu dokumentieren, aktuell zu halten und den zuständigen Organisationseinheiten zugänglich zu machen.

Art. 99 Wirksamkeitsbewertung

Die Wirksamkeit der Schulungs- und Sensibilisierungsmaßnahmen ist regelmäßig zu überprüfen.

Hierbei sind insbesondere zu berücksichtigen:

- Schulungsstand;
- Rückmeldungen der Teilnehmenden;
- Datenschutzvorfälle;
- Auditfeststellungen;
- Verbesserungsmaßnahmen.

Art. 100 Dokumentation

Alle Schulungen, Sensibilisierungsmaßnahmen und Qualifikationsnachweise sind vollständig, nachvollziehbar und revisionssicher zu dokumentieren.

Kapitel 11 – Dokumentation, Datenschutzregister und Nachweisführung

---

Art. 101 Grundsatz

Die Yushin-Ryu AG dokumentiert sämtliche datenschutzrelevanten Prozesse, Entscheidungen und Maßnahmen vollständig, nachvollziehbar und revisionssicher.

Die Dokumentation dient dem Nachweis der Einhaltung gesetzlicher Anforderungen sowie der kontinuierlichen Verbesserung des Datenschutzmanagementsystems.

Art. 102 Datenschutzdokumentation

Die Gesellschaft führt eine zentrale Datenschutzdokumentation.

Diese umfasst insbesondere:

- Datenschutzreglemente;
- Richtlinien;
- Weisungen;
- Prozesse;
- Verfahrensanweisungen;
- Schulungsunterlagen;
- Prüfberichte.

Art. 103 Verzeichnis der Verarbeitungstätigkeiten

Die Gesellschaft führt ein zentrales Verzeichnis sämtlicher datenschutzrelevanter Verarbeitungstätigkeiten.

Dieses enthält mindestens:

- Bezeichnung der Verarbeitung;
- verantwortliche Organisationseinheit;
- Zweck der Verarbeitung;
- Kategorien personenbezogener Daten;
- Kategorien betroffener Personen;
- Empfänger der Daten;
- Aufbewahrungsfristen;
- technische und organisatorische Schutzmaßnahmen.

Art. 104 Datenschutzregister

Die Datenschutzfunktion führt ein zentrales Datenschutzregister.

Dieses umfasst insbesondere:

- Datenschutzvorfälle;
- Datenschutz-Folgenabschätzungen;
- Betroffenenanfragen;
- Einwilligungen;
- Auftragsbearbeitungen;
- internationale Datenübermittlungen;
- interne Datenschutzprüfungen.

Art. 105 Nachweispflicht

Die Yushin-Ryu AG weist die Einhaltung datenschutzrechtlicher Anforderungen durch geeignete Dokumentationen und Nachweise nach.

Hierzu gehören insbesondere:

- Verfahrensdokumentationen;
- Protokolle;
- Freigaben;
- Prüfberichte;
- Auditberichte;
- Schulungsnachweise.

Art. 106 Versionierung

Datenschutzrelevante Dokumente unterliegen einer geregelten Versionierung.

Änderungen sind nachvollziehbar zu dokumentieren.

Die Versionshistorie enthält mindestens:

- Versionsnummer;
- Änderungsdatum;
- Beschreibung der Änderung;
- verantwortliche Person;
- Genehmigungsdatum.

Art. 107 Aufbewahrung

Datenschutzrelevante Unterlagen sind entsprechend den gesetzlichen Aufbewahrungsfristen sowie den internen Archivierungsregelungen aufzubewahren.

Art. 108 Archivierung

Die Archivierung erfolgt nach den Grundsätzen:

- Vollständigkeit;
- Integrität;
- Authentizität;
- Verfügbarkeit;
- Nachvollziehbarkeit.

Elektronische Dokumente sind gegen Verlust, Manipulation und unbefugten Zugriff zu schützen.

Art. 109 Datenschutzkennzahlen

Zur Steuerung des Datenschutzmanagementsystems können geeignete Datenschutzkennzahlen (Key Privacy Indicators – KPI) erhoben und ausgewertet werden.

Hierzu gehören insbesondere:

- Anzahl der Datenschutzvorfälle;

- Bearbeitungsdauer von Betroffenenanfragen;
- Schulungsquote;
- Ergebnisse interner Audits;
- Status offener Maßnahmen.

Art. 110 Regelmäßige Überprüfung

Die Datenschutzdokumentation sowie das Datenschutzregister sind regelmäßig auf Aktualität, Vollständigkeit und Qualität zu überprüfen.

Festgestellte Mängel sind zeitnah zu beheben.

Kapitel 12 – Datenschutz-Audits, Überwachung und kontinuierliche Verbesserung

---

Art. 111 Grundsatz

Die Yushin-Ryu AG überprüft die Wirksamkeit ihres Datenschutzmanagementsystems regelmäßig durch interne und externe Audits sowie durch geeignete Überwachungs- und Kontrollmaßnahmen.

Art. 112 Zielsetzung

Die Datenschutz-Audits dienen insbesondere:

- der Überprüfung der Einhaltung gesetzlicher Anforderungen;
- der Bewertung der Wirksamkeit des Datenschutzmanagementsystems;
- der Identifikation von Verbesserungspotenzialen;
- der Unterstützung der Corporate Governance;
- der kontinuierlichen Verbesserung.

Art. 113 Auditplanung

Die Datenschutzfunktion erstellt einen risikoorientierten Auditplan.

Hierbei sind insbesondere zu berücksichtigen:

- Ergebnisse früherer Audits;
- Datenschutzrisiken;
- Datenschutzvorfälle;
- neue Prozesse;
- neue Systeme;
- organisatorische Veränderungen.

Art. 114 Interne Datenschutz-Audits

Interne Datenschutz-Audits werden regelmäßig durchgeführt.

Sie umfassen insbesondere:

- Organisation;
- Personal;
- IT;
- Forschung;
- Lehre;
- Studierendenverwaltung;
- internationale Datenverarbeitung;
- Auftragsbearbeitungen.

Art. 115 Externe Datenschutz-Audits

Soweit erforderlich oder gesetzlich vorgesehen, können externe Datenschutzprüfungen oder Audits durchgeführt werden.

Die Ergebnisse fließen in die Weiterentwicklung des Datenschutzmanagementsystems ein.

Art. 116 Auditfeststellungen

Festgestellte Abweichungen sind nach ihrer Bedeutung zu bewerten.

Für sämtliche wesentlichen Feststellungen sind geeignete Maßnahmen einschließlich Verantwortlichkeiten und Umsetzungsfristen festzulegen.

Art. 117 Maßnahmenverfolgung

Die Umsetzung beschlossener Maßnahmen ist regelmäßig zu überwachen.

Offene Maßnahmen sind bis zu ihrem Abschluss nachzuverfolgen und hinsichtlich ihrer Wirksamkeit zu bewerten.

Art. 118 Managementbewertung

Die Ergebnisse der Datenschutz-Audits werden mindestens einmal jährlich im Rahmen des Management Reviews bewertet.

Hierbei sind insbesondere zu berücksichtigen:

- Datenschutzvorfälle;
- Auditfeststellungen;
- Schulungsstand;
- Betroffenenanfragen;
- gesetzliche Änderungen;
- Verbesserungsmaßnahmen.

Art. 119 Kontinuierliche Verbesserung

Das Datenschutzmanagementsystem wird regelmäßig weiterentwickelt.

Neue gesetzliche Anforderungen, technische Entwicklungen sowie organisatorische Veränderungen sind angemessen zu berücksichtigen.

Art. 120 Berichtswesen

Die Datenschutzfunktion berichtet regelmäßig an die Geschäftsleitung über:

- den Stand des Datenschutzmanagementsystems;
- wesentliche Datenschutzrisiken;
- Ergebnisse der Datenschutz-Audits;
- offene Maßnahmen;
- Datenschutzvorfälle;
- Verbesserungspotenziale.

Kapitel 13 – Governance, Management Review und strategische Steuerung des Datenschutzes

---

Art. 121 Grundsatz

Der Datenschutz ist ein integraler Bestandteil der Corporate Governance der Yushin-Ryu AG.

Er unterstützt den Verwaltungsrat sowie die Geschäftsleitung bei der rechtskonformen, verantwortungsvollen und nachhaltigen Unternehmensführung.

Art. 122 Strategische Steuerung

Die strategische Steuerung des Datenschutzmanagements erfolgt durch den Verwaltungsrat in Zusammenarbeit mit dem CVO, dem CEO sowie der zuständigen Datenschutzfunktion.

Hierbei sind insbesondere zu berücksichtigen:

- Unternehmensstrategie;
- internationale Entwicklung;
- Digitalisierung;
- Forschungsstrategie;
- Informationssicherheit;
- Qualitätsmanagement;
- Risikomanagement;
- gesetzliche Entwicklungen.

Art. 123 Management Review

Das Datenschutzmanagementsystem ist mindestens einmal jährlich im Rahmen eines Management Reviews umfassend zu bewerten.

Zusätzliche Management Reviews sind insbesondere durchzuführen bei:

- wesentlichen Datenschutzvorfällen;
- erheblichen organisatorischen Änderungen;
- Einführung neuer Technologien;
- Änderungen gesetzlicher Anforderungen;
- wesentlichen Auditfeststellungen.

Art. 124 Bewertungsgrundlagen

Im Management Review sind insbesondere zu bewerten:

- Wirksamkeit des Datenschutzmanagementsystems;
- Ergebnisse interner und externer Audits;

- Datenschutzvorfälle;
- Betroffenenanfragen;
- Datenschutz-Folgenabschätzungen;
- Schulungsstand;
- offene Maßnahmen;
- Verbesserungspotenziale.

Art. 125 Strategischer Datenschutzbericht

Die Datenschutzfunktion erstellt mindestens einmal jährlich einen strategischen Datenschutzbericht.

Dieser enthält insbesondere:

- Stand des Datenschutzmanagementsystems;
- Datenschutzrisiken;
- Datenschutzvorfälle;
- Auditfeststellungen;
- Entwicklungsbedarf;
- Handlungsempfehlungen.

Art. 126 Entscheidungsgrundlagen

Der strategische Datenschutzbericht dient dem Verwaltungsrat sowie der Geschäftsleitung als Grundlage für strategische Entscheidungen.

Hierzu gehören insbesondere:

- Organisationsentwicklung;
- Digitalisierung;
- internationale Projekte;
- Investitionen;
- Forschungsvorhaben;
- Informationssicherheit.

Art. 127 Zusammenarbeit mit anderen Managementsystemen

Das Datenschutzmanagement arbeitet eng zusammen mit:

- Qualitätsmanagement;
- Compliance;
- Risikomanagement;

- Informationssicherheitsmanagement;
- Internem Kontrollsystem (IKS);
- Business Continuity Management;
- Personalmanagement;
- Forschungsmanagement.

Art. 128 Datenschutz-Governance

Die Datenschutz-Governance richtet sich insbesondere nach folgenden Grundsätzen:

- Rechtmäßigkeit;
- Transparenz;
- Verantwortlichkeit;
- Integrität;
- Verhältnismäßigkeit;
- Nachvollziehbarkeit;
- kontinuierliche Verbesserung.

Art. 129 Internationale Datenverarbeitung

Bei internationalen Verarbeitungsvorgängen sind sowohl die internen Datenschutzstandards der Yushin-Ryu AG als auch die jeweils anwendbaren gesetzlichen Datenschutzvorschriften zu berücksichtigen.

Die datenschutzrechtlichen Anforderungen sind bereits in der Planungsphase internationaler Projekte zu bewerten.

Art. 130 Kontinuierliche Weiterentwicklung

Das Datenschutzmanagementsystem wird regelmäßig an neue gesetzliche Anforderungen, internationale Entwicklungen, technologische Veränderungen sowie organisatorische Bedürfnisse angepasst.

Kapitel 14 – Zusammenarbeit mit Behörden, Aufsichts- und Akkreditierungsstellen

Art. 131 Grundsatz

Die Yushin-Ryu AG arbeitet im Bereich des Datenschutzes vertrauensvoll, transparent und rechtskonform mit den zuständigen Behörden, Aufsichts-, Prüfungs-, Zertifizierungs- und Akkreditierungsstellen zusammen.

Die Unabhängigkeit der jeweiligen Stellen bleibt jederzeit gewahrt.

Art. 132 Zusammenarbeit mit Datenschutzaufsichtsbehörden

Die Gesellschaft unterstützt die zuständigen Datenschutzaufsichtsbehörden im Rahmen ihrer gesetzlichen Aufgaben.

Erforderliche Auskünfte und Unterlagen sind vollständig, wahrheitsgemäß und fristgerecht bereitzustellen.

Art. 133 Zusammenarbeit mit Akkreditierungsstellen

Soweit Datenschutz Bestandteil institutioneller oder programmbezogener Akkreditierungsverfahren ist, stellt die Gesellschaft die erforderlichen Nachweise zur Verfügung.

Hierzu gehören insbesondere:

- Datenschutzorganisation;
- Datenschutzprozesse;
- Datenschutzmanagementsystem;
- Schulungsnachweise;
- Auditberichte;
- Management Reviews;
- Dokumentationen.

Art. 134 Zusammenarbeit mit Zertifizierungsstellen

Die Gesellschaft unterstützt Datenschutzprüfungen im Rahmen freiwilliger oder gesetzlich vorgesehener Zertifizierungsverfahren.

Feststellungen und Empfehlungen sind angemessen zu bewerten und in die Weiterentwicklung des Datenschutzmanagementsystems einzubeziehen.

Art. 135 Zusammenarbeit mit Revisionsstellen

Interne und externe Revisionsstellen erhalten im Rahmen ihrer gesetzlichen oder vertraglichen Aufgaben Zugang zu den erforderlichen datenschutzrelevanten Informationen.

Der Datenschutz sowie gesetzliche Geheimhaltungspflichten bleiben hierbei gewahrt.

Art. 136 Behördenkommunikation

Die Kommunikation mit Behörden erfolgt ausschließlich durch die hierfür zuständigen oder ausdrücklich bevollmächtigten Stellen.

Sämtliche behördlichen Anfragen und Verfahren sind nachvollziehbar zu dokumentieren.

Art. 137 Mitwirkungspflichten

Alle Organisationseinheiten sind verpflichtet, Datenschutzprüfungen sowie behördliche Verfahren aktiv zu unterstützen.

Erforderliche Informationen sind vollständig und fristgerecht bereitzustellen.

Art. 138 Vertraulichkeit

Auch gegenüber Behörden, Prüfungs- und Akkreditierungsstellen dürfen personenbezogene Daten ausschließlich im gesetzlich zulässigen Umfang offengelegt werden.

Der Grundsatz der Datenminimierung ist zu beachten.

Art. 139 Dokumentation

Sämtliche Prüfungen, Stellungnahmen, Behördenkontakte sowie Maßnahmen sind vollständig, nachvollziehbar und revisionssicher zu dokumentieren.

Art. 140 Kontinuierliche Verbesserung

Erkenntnisse aus behördlichen Verfahren, Akkreditierungen, Zertifizierungen sowie internen und externen Prüfungen sind systematisch auszuwerten.

Geeignete Verbesserungsmaßnahmen sind zeitnah umzusetzen.

Kapitel 15 – Internationale Datenverarbeitung und grenzüberschreitender Datenschutz

Art. 141 Grundsatz

Die Yushin-Ryu AG gewährleistet bei internationalen Datenverarbeitungen ein angemessenes Datenschutzniveau.

Grenzüberschreitende Datenverarbeitungen erfolgen ausschließlich unter Einhaltung der anwendbaren gesetzlichen Vorschriften sowie der internen Datenschutzstandards der Gesellschaft.

Art. 142 Zielsetzung

Die internationale Datenverarbeitung dient insbesondere:

- der Unterstützung internationaler Forschungsprojekte;
- der Zusammenarbeit mit Hochschulen und Forschungseinrichtungen;
- der internationalen Verwaltung;
- der Erfüllung gesetzlicher Verpflichtungen;
- der sicheren Durchführung internationaler Geschäftsprozesse.

Art. 143 Internationale Datenübermittlungen

Vor jeder grenzüberschreitenden Übermittlung personenbezogener Daten ist zu prüfen:

- die Rechtsgrundlage der Übermittlung;
- das Datenschutzniveau des Empfängerstaates;
- geeignete Schutzmaßnahmen;
- vertragliche Verpflichtungen;
- organisatorische Sicherheitsmaßnahmen.

Die Ergebnisse der Prüfung sind zu dokumentieren.

Art. 144 Internationale Kooperationen

Bei internationalen Kooperationen sind datenschutzrechtliche Verantwortlichkeiten vor Beginn der Zusammenarbeit schriftlich festzulegen.

Hierbei sind insbesondere zu regeln:

- Verantwortlichkeiten;
- Datenzugriffe;
- Datenübermittlungen;
- Löschfristen;
- Sicherheitsmaßnahmen;
- Meldewege bei Datenschutzverletzungen.

Art. 145 Internationale Forschungsprojekte

Internationale Forschungsprojekte mit personenbezogenen Daten unterliegen einer datenschutzrechtlichen Prüfung vor Projektbeginn.

Dabei sind insbesondere zu berücksichtigen:

- Forschungszweck;
- Art der Daten;
- betroffene Personengruppen;
- internationale Datenflüsse;
- gesetzliche Anforderungen der beteiligten Staaten.

Art. 146 Cloud- und Hosting-Dienstleistungen

Werden personenbezogene Daten in Cloud-Systemen oder externen Rechenzentren verarbeitet, sind insbesondere zu prüfen:

- Standort der Datenverarbeitung;
- Sicherheitsmaßnahmen;
- Zugriffsberechtigungen;
- Auftragsbearbeitung;
- Notfallkonzepte;
- vertragliche Datenschutzregelungen.

Art. 147 Internationale Standorte

Alle internationalen Standorte der Yushin-Ryu AG sind verpflichtet, dieses Datenschutzreglement einzuhalten.

Zusätzlich sind die jeweils anwendbaren gesetzlichen Datenschutzvorschriften des betreffenden Staates zu beachten.

Art. 148 Internationale Audits

Internationale Standorte sind regelmäßig in das Datenschutz-Auditprogramm einzubeziehen.

Erforderlichenfalls können ergänzende externe Datenschutzprüfungen durchgeführt werden.

Art. 149 Berichtswesen

Die Datenschutzfunktion berichtet regelmäßig über wesentliche internationale Datenschutzthemen.

Hierzu gehören insbesondere:

- internationale Datenübermittlungen;
- Datenschutzrisiken;
- internationale Datenschutzvorfälle;
- Auditfeststellungen;
- Verbesserungsmaßnahmen.

Art. 150 Abschluss des Kapitels

Die internationale Datenverarbeitung erfolgt unter Berücksichtigung der strategischen Ausrichtung der Yushin-Ryu AG sowie der jeweils anwendbaren gesetzlichen Datenschutzanforderungen.

Sie trägt zur sicheren und rechtskonformen Zusammenarbeit mit nationalen und internationalen Partnern bei.

Kapitel 16 – Forschung, Lehre und wissenschaftliche Datenverarbeitung

---

Art. 151 Grundsatz

Die Verarbeitung personenbezogener Daten in Forschung und Lehre erfolgt unter Beachtung der wissenschaftlichen Freiheit sowie der anwendbaren datenschutzrechtlichen Vorschriften.

Der Schutz der Persönlichkeitsrechte betroffener Personen ist jederzeit sicherzustellen.

Art. 152 Zielsetzung

Die Verarbeitung personenbezogener Daten im wissenschaftlichen Bereich dient insbesondere:

- der Durchführung von Forschungsvorhaben;
- der Durchführung der Lehre;
- der Betreuung von Studierenden;
- der wissenschaftlichen Dokumentation;
- der Qualitätssicherung;
- der Förderung wissenschaftlicher Erkenntnisse.

Art. 153 Verarbeitung personenbezogener Forschungsdaten

Personenbezogene Forschungsdaten dürfen ausschließlich verarbeitet werden, soweit dies für das jeweilige Forschungsvorhaben erforderlich ist.

Der Umfang der Verarbeitung ist auf das notwendige Maß zu beschränken.

Art. 154 Pseudonymisierung und Anonymisierung

Soweit wissenschaftlich möglich und rechtlich zulässig, sind personenbezogene Daten vor ihrer weiteren Verarbeitung zu pseudonymisieren oder zu anonymisieren.

Die Wahl der geeigneten Methode ist zu dokumentieren.

Art. 155 Forschungsprojekte

Vor Beginn eines Forschungsvorhabens mit personenbezogenen Daten sind insbesondere zu prüfen:

- Forschungszweck;
- Rechtsgrundlage;
- Datenkategorien;

- Schutzmaßnahmen;
- Speicherdauer;
- Löschkonzept;
- datenschutzrechtliche Risiken.

Art. 156 Ethik und Datenschutz

Soweit Forschungsvorhaben einer Ethikprüfung unterliegen, sind Datenschutz und ethische Anforderungen gemeinsam zu berücksichtigen.

Die zuständigen Gremien arbeiten hierbei eng zusammen.

Art. 157 Studierendendaten

Personenbezogene Daten von Studierenden dürfen ausschließlich für Aufgaben verwendet werden, welche im Zusammenhang mit Studium, Lehre, Prüfungen, Betreuung oder gesetzlichen Verpflichtungen stehen.

Art. 158 Wissenschaftliche Veröffentlichungen

Bei wissenschaftlichen Veröffentlichungen sind personenbezogene Daten nur zu verwenden, soweit hierfür eine gesetzliche Grundlage besteht oder die betroffene Person eingewilligt hat.

Soweit möglich, sind Daten vor der Veröffentlichung zu anonymisieren.

Art. 159 Forschungskooperationen

Werden personenbezogene Daten im Rahmen wissenschaftlicher Kooperationen verarbeitet, sind Verantwortlichkeiten sowie datenschutzrechtliche Anforderungen vor Beginn der Zusammenarbeit schriftlich festzulegen.

Art. 160 Archivierung wissenschaftlicher Daten

Wissenschaftliche Daten sind entsprechend den gesetzlichen Vorgaben sowie den internen Archivierungsregelungen aufzubewahren.

Personenbezogene Daten sind nach Ablauf der Aufbewahrungsfristen zu löschen oder zu anonymisieren, sofern keine gesetzlichen oder wissenschaftlichen Gründe entgegenstehen.

Kapitel 17 – Aufbewahrung, Löschung und Datenvernichtung

Art. 161 Grundsatz

Personenbezogene Daten sind nur so lange aufzubewahren, wie dies zur Erfüllung des jeweiligen Verarbeitungszwecks, aufgrund gesetzlicher Aufbewahrungspflichten oder aufgrund berechtigter Interessen erforderlich ist.

Nach Ablauf der jeweiligen Fristen sind die Daten datenschutzkonform zu löschen, zu anonymisieren oder – soweit gesetzlich zulässig – zu vernichten.

Art. 162 Aufbewahrungsfristen

Für sämtliche Kategorien personenbezogener Daten sind angemessene Aufbewahrungsfristen festzulegen.

Hierbei sind insbesondere zu berücksichtigen:

- gesetzliche Aufbewahrungspflichten;
- vertragliche Verpflichtungen;
- wissenschaftliche Anforderungen;
- Akkreditierungsanforderungen;
- Archivierungsregelungen der Gesellschaft.

Art. 163 Löschkonzepte

Die Gesellschaft erstellt und unterhält dokumentierte Löschkonzepte.

Diese regeln insbesondere:

- Verantwortlichkeiten;
- Löschfristen;
- Löschverfahren;
- Kontrollmechanismen;
- Dokumentation.

Art. 164 Regelmäßige Überprüfung

Gespeicherte personenbezogene Daten sind regelmäßig darauf zu überprüfen, ob ihre weitere Speicherung noch erforderlich ist.

Nicht mehr benötigte Daten sind entsprechend den geltenden Regelungen zu löschen oder zu anonymisieren.

Art. 165 Sichere Löschung

Personenbezogene Daten sind durch geeignete technische und organisatorische Maßnahmen so zu löschen, dass eine Wiederherstellung mit vertretbarem Aufwand ausgeschlossen ist.

Art. 166 Vernichtung physischer Datenträger

Datenträger in Papierform oder sonstige physische Speichermedien mit personenbezogenen Daten sind nach anerkannten Sicherheitsverfahren zu vernichten.

Die Vernichtung ist nachvollziehbar zu dokumentieren.

Art. 167 Vernichtung elektronischer Datenträger

Elektronische Datenträger sind vor ihrer Entsorgung oder Weitergabe nach anerkannten Verfahren sicher zu löschen oder zu zerstören.

Soweit erforderlich, ist die Vernichtung nachzuweisen.

Art. 168 Archivierung

Archivierungspflichtige Unterlagen sind entsprechend den gesetzlichen Anforderungen sowie den internen Archivierungsregelungen aufzubewahren.

Der Zugriff auf archivierte personenbezogene Daten ist auf berechtigte Personen zu beschränken.

Art. 169 Aussetzung der Löschung

Bestehen gesetzliche, gerichtliche oder behördliche Gründe, welche einer Löschung entgegenstehen, ist die Löschung bis zum Wegfall dieser Gründe auszusetzen.

Die Gründe für die Aussetzung sind zu dokumentieren.

Art. 170 Kontrolle und Nachweis

Die Einhaltung der Aufbewahrungs-, Lösch- und Vernichtungsregelungen ist regelmäßig zu überprüfen.

Die Durchführung wesentlicher Lösch- und Vernichtungsmaßnahmen ist nachvollziehbar zu dokumentieren.

Kapitel 18 – Datenschutz im Personalwesen

Art. 171 Grundsatz

Die Verarbeitung personenbezogener Daten von Bewerberinnen und Bewerbern, Mitarbeitenden, Organmitgliedern, Dozierenden sowie weiteren Beschäftigten erfolgt ausschließlich im Rahmen der gesetzlichen Bestimmungen sowie dieses Reglements.

Dabei sind die Persönlichkeitsrechte der betroffenen Personen jederzeit zu schützen.

Art. 172 Bewerbungsverfahren

Personenbezogene Daten im Rahmen von Bewerbungsverfahren dürfen ausschließlich zum Zweck der Durchführung des Auswahl- und Einstellungsverfahrens verarbeitet werden.

Nicht mehr benötigte Bewerbungsunterlagen sind entsprechend den gesetzlichen Vorgaben zu löschen oder zurückzugeben.

Art. 173 Personalakten

Für jede Mitarbeiterin und jeden Mitarbeiter kann eine Personalakte geführt werden.

Der Zugriff ist ausschließlich den hierzu berechtigten Personen gestattet.

Art. 174 Vertraulichkeit

Personalakten sowie personenbezogene Beschäftigtendaten sind vertraulich zu behandeln.

Eine Weitergabe erfolgt ausschließlich auf gesetzlicher Grundlage oder im Rahmen der dienstlichen Erforderlichkeit.

Art. 175 Zugriffsberechtigungen

Zugriffsrechte auf personenbezogene Beschäftigtendaten sind nach dem Need-to-know-Prinzip zu vergeben.

Die Berechtigungen sind regelmäßig zu überprüfen und bei organisatorischen Änderungen anzupassen.

Art. 176 Leistungs- und Qualifikationsdaten

Daten über Qualifikationen, Fortbildungen, Beurteilungen und Leistungsnachweise dürfen ausschließlich für Personalentwicklung, gesetzliche Verpflichtungen sowie personalbezogene Verwaltungszwecke verwendet werden.

Art. 177 Gesundheitsdaten

Gesundheitsdaten sowie andere besonders schützenswerte Personendaten von Beschäftigten unterliegen erhöhten Datenschutzanforderungen.

Sie dürfen ausschließlich von hierzu berechtigten Stellen verarbeitet werden.

Art. 178 Elektronische Personalverwaltung

Elektronische Personalverwaltungssysteme sind durch angemessene technische und organisatorische Maßnahmen gegen unbefugten Zugriff, Verlust oder Manipulation zu schützen.

Art. 179 Aufbewahrung und Löschung

Personenbezogene Beschäftigtendaten sind entsprechend den gesetzlichen Aufbewahrungsfristen sowie den internen Archivierungsregelungen aufzubewahren.

Nach Ablauf der Fristen sind sie datenschutzkonform zu löschen oder zu anonymisieren, sofern keine gesetzlichen Gründe entgegenstehen.

Art. 180 Datenschutz im Personalmanagement

Das Personalmanagement überprüft regelmäßig die Einhaltung der datenschutzrechtlichen Anforderungen innerhalb sämtlicher personalbezogener Prozesse.

Festgestellte Mängel sind zeitnah zu beheben.

Kapitel 19 – Datenschutz in IT-Systemen und digitalen Diensten

Art. 181 Grundsatz

Alle IT-Systeme, Anwendungen, digitalen Dienste sowie Informations- und Kommunikationssysteme der Yushin-Ryu AG sind so zu betreiben, dass der Schutz personenbezogener Daten jederzeit gewährleistet ist.

Datenschutz und Informationssicherheit sind bereits bei der Planung, Entwicklung, Beschaffung, Einführung und dem Betrieb zu berücksichtigen.

Art. 182 Datenschutz bei der Systementwicklung

Neue IT-Systeme, Softwarelösungen und digitale Anwendungen sind bereits während ihrer Entwicklung nach den Grundsätzen des Datenschutzes und der Informationssicherheit zu konzipieren.

Datenschutzanforderungen sind frühzeitig in den Entwicklungsprozess einzubeziehen.

Art. 183 Benutzer- und Berechtigungsmanagement

Für sämtliche IT-Systeme ist ein dokumentiertes Benutzer- und Berechtigungskonzept zu führen.

Zugriffsrechte werden ausschließlich nach dem Need-to-know- und Least-Privilege-Prinzip vergeben.

Berechtigungen sind regelmäßig zu überprüfen und bei personellen oder organisatorischen Änderungen unverzüglich anzupassen.

Art. 184 Authentifizierung

Der Zugriff auf Systeme mit personenbezogenen Daten erfolgt ausschließlich durch geeignete Authentifizierungsverfahren.

Für Systeme mit erhöhtem Schutzbedarf sind zusätzliche Authentifizierungsmaßnahmen vorzusehen.

Art. 185 Protokollierung

Datenschutzrelevante Zugriffe, Änderungen und administrative Tätigkeiten sind entsprechend den gesetzlichen Vorgaben sowie den internen Sicherheitsregelungen zu protokollieren.

Protokolldaten sind gegen Manipulation zu schützen und ausschließlich berechtigten Personen zugänglich zu machen.

Art. 186 Mobile Endgeräte und mobiles Arbeiten

Werden personenbezogene Daten über mobile Endgeräte oder im Rahmen mobiler Arbeitsformen verarbeitet, sind geeignete technische und organisatorische Schutzmaßnahmen anzuwenden.

Insbesondere sind Vorgaben zur Zugriffssicherung, Verschlüsselung sowie zum Schutz vor Verlust oder Diebstahl einzuhalten.

Art. 187 Cloud-Dienste und digitale Plattformen

Cloud-Dienste, Software-as-a-Service-Lösungen sowie digitale Plattformen dürfen nur eingesetzt werden, wenn die datenschutzrechtlichen, informationssicherheitsrechtlichen und vertraglichen Anforderungen erfüllt sind.

Vor ihrer Einführung ist eine entsprechende Prüfung durchzuführen.

Art. 188 Künstliche Intelligenz und automatisierte Verarbeitung

Beim Einsatz künstlicher Intelligenz sowie automatisierter Entscheidungs- und Verarbeitungssysteme sind Datenschutz, Transparenz, Nachvollziehbarkeit und menschliche Aufsicht angemessen sicherzustellen.

Der Einsatz ist vor seiner Einführung hinsichtlich datenschutzrechtlicher Risiken zu bewerten.

Art. 189 Zusammenarbeit mit der Informationssicherheit

Die Datenschutzfunktion arbeitet eng mit dem Informationssicherheitsmanagement sowie dem Chief Information Security Officer (CISO) zusammen.

Datenschutz- und Informationssicherheitsmaßnahmen sind aufeinander abzustimmen und regelmäßig gemeinsam zu überprüfen.

Art. 190 Kontinuierliche Weiterentwicklung

Die datenschutzrechtlichen Anforderungen an IT-Systeme und digitale Dienste sind regelmäßig an neue gesetzliche Vorgaben, technologische Entwicklungen sowie interne Sicherheitsanforderungen anzupassen.

Kapitel 20 – Strategische Weiterentwicklung des Datenschutzmanagements

---

Art. 191 Grundsatz

Die Yushin-Ryu AG entwickelt ihr Datenschutzmanagementsystem kontinuierlich weiter.

Dabei sind gesetzliche Entwicklungen, internationale Anforderungen, technologische Innovationen sowie organisatorische Veränderungen systematisch zu berücksichtigen.

Art. 192 Strategische Weiterentwicklung

Der Datenschutz ist Bestandteil der langfristigen Unternehmensstrategie.

Er ist frühzeitig in strategische Entscheidungen, Organisationsentwicklungen, Digitalisierungsprojekte sowie nationale und internationale Vorhaben einzubeziehen.

Art. 193 Datenschutzstrategie

Die Gesellschaft erstellt und überprüft regelmäßig eine Datenschutzstrategie.

Diese berücksichtigt insbesondere:

- Unternehmensentwicklung;
- Digitalisierung;
- Forschung;
- Lehre;
- internationale Standorte;
- Informationssicherheit;
- Qualitätsmanagement;
- Risikomanagement.

Art. 194 Innovationsmanagement

Neue Technologien, Verfahren und digitale Anwendungen sind hinsichtlich ihrer datenschutzrechtlichen Auswirkungen vor ihrer Einführung zu bewerten.

Geeignete Schutzmaßnahmen sind frühzeitig festzulegen und regelmäßig zu überprüfen.

Art. 195 Kennzahlen und Leistungsbewertung

Zur Steuerung des Datenschutzmanagementsystems können geeignete Kennzahlen erhoben und ausgewertet werden.

Hierzu gehören insbesondere:

- Datenschutzvorfälle;
- Bearbeitungszeiten;
- Schulungsquote;
- Auditfeststellungen;
- Umsetzungsgrad von Verbesserungsmaßnahmen;
- Ergebnisse interner Überprüfungen.

Art. 196 Zusammenarbeit mit dem integrierten Managementsystem

Das Datenschutzmanagement ist Bestandteil des integrierten Managementsystems der Yushin-Ryu AG.

Es arbeitet insbesondere mit folgenden Managementsystemen zusammen:

- Qualitätsmanagement;
- Risikomanagement;
- Compliance-Management;
- Informationssicherheitsmanagement;
- Internes Kontrollsystem (IKS);
- Business Continuity Management;
- Governance-System.

Art. 197 Managementbewertung

Die oberste Leitung bewertet regelmäßig die Wirksamkeit des Datenschutzmanagementsystems.

Hierbei sind insbesondere zu berücksichtigen:

- Ergebnisse interner und externer Audits;
- Datenschutzvorfälle;
- gesetzliche Änderungen;
- Zielerreichung;
- Ressourcenbedarf;
- Verbesserungspotenziale.

Art. 198 Internationale Entwicklungen

Internationale Entwicklungen im Datenschutz sind fortlaufend zu beobachten.

Soweit erforderlich, sind interne Regelungen an neue rechtliche, technische oder organisatorische Anforderungen anzupassen.

Art. 199 Kontinuierliche Verbesserung

Die kontinuierliche Verbesserung erfolgt auf Grundlage von:

- Audits;

- Management Reviews;
- Risikoanalysen;
- Datenschutzvorfällen;
- Lessons Learned;
- gesetzlichen Änderungen;
- Rückmeldungen der Organisationseinheiten;
- Verbesserungsvorschlägen.

Art. 200 Abschluss des Kapitels

Die kontinuierliche Weiterentwicklung des Datenschutzmanagementsystems gewährleistet den langfristigen Schutz personenbezogener Daten sowie die nachhaltige Unterstützung von Forschung, Lehre, Verwaltung und internationalen Aktivitäten der Yushin-Ryu AG.

Kapitel 21 – Schlussbestimmungen

Art. 201 Grundsatz

Dieses Datenschutzreglement bildet gemeinsam mit den Statuten sowie den übrigen Reglementen der Yushin-Ryu AG die verbindliche Grundlage des Datenschutzmanagementsystems.

Es ist von sämtlichen Organen, Führungskräften, Mitarbeitenden sowie weiteren von diesem Reglement erfassten Personen einzuhalten.

Art. 202 Verhältnis zu anderen Reglementen

Dieses Reglement ergänzt insbesondere:

- Organisationsreglement;
- Personalreglement;
- Finanzreglement;
- Kompetenzreglement;
- Qualitätsmanagement-Reglement;
- Risikomanagement-Reglement;
- Compliance-Reglement;
- Informationssicherheitsreglement;
- Forschungs- und Laborsicherheitsreglement;
- weitere durch den Verwaltungsrat erlassene Reglemente.

Bei Widersprüchen gehen zwingende gesetzliche Vorschriften sowie die Statuten der Gesellschaft vor.

Art. 203 Verbindlichkeit

Die Einhaltung dieses Datenschutzreglements ist Bestandteil der Corporate Governance der Yushin-Ryu AG.

Verstöße gegen dieses Reglement können arbeits-, zivil-, verwaltungs- oder strafrechtliche Folgen nach sich ziehen, soweit dies gesetzlich vorgesehen ist.

Art. 204 Regelmäßige Überprüfung

Dieses Reglement ist mindestens einmal jährlich auf Aktualität, Vollständigkeit und Wirksamkeit zu überprüfen.

Eine außerordentliche Überprüfung erfolgt insbesondere bei:

- Änderungen der Datenschutzgesetzgebung;
- wesentlichen organisatorischen Änderungen;
- erheblichen Datenschutzvorfällen;
- Änderungen der Unternehmensstruktur;
- Ergebnissen interner oder externer Audits;
- Beschlüssen des Verwaltungsrates.

Art. 205 Änderungen

Änderungen dieses Reglements bedürfen der Genehmigung durch den Verwaltungsrat.

Alle Änderungen sind nachvollziehbar zu dokumentieren und gemäß den Vorgaben der Dokumentenlenkung zu versionieren.

Art. 206 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Reglements ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

An die Stelle der unwirksamen Bestimmung tritt eine Regelung, welche dem Zweck der ursprünglichen Bestimmung möglichst nahekommt.

Art. 207 Sprachfassungen

Werden mehrere Sprachfassungen dieses Reglements erstellt, bestimmt der Verwaltungsrat die verbindliche Originalfassung.

Übersetzungen dienen der internationalen Anwendung und Information.

Art. 208 Inkrafttreten

Dieses Datenschutzreglement tritt nach Genehmigung durch den Verwaltungsrat am festgelegten Datum in Kraft.

Mit seinem Inkrafttreten ersetzt es sämtliche früheren Fassungen dieses Reglements.

Art. 209 Übergangsbestimmungen

Bestehende Prozesse, Richtlinien und Weisungen sind innerhalb angemessener Fristen an dieses Reglement anzupassen.

Bereits begründete Rechte und Pflichten bleiben hiervon unberührt.

Art. 210 Schlussbestimmung

Dieses Datenschutzreglement bildet die verbindliche Grundlage für den Schutz personenbezogener Daten innerhalb der Yushin-Ryu AG.

Es unterstützt eine rechtskonforme, verantwortungsbewusste und transparente Datenverarbeitung und trägt zur nachhaltigen Sicherung von Forschung, Lehre, Verwaltung und internationalen Kooperationen bei.