Datenschutzverwaltung

Datum	02.11.17	**Revision:**	1.0	**Nr.:**	PS_OBJ5.1

Bereich	Sicherheit von Informationssystemen – Datenschutzverwaltung
Referenz	PS_OBJ 5.1 bezieht sich auf die Nomenklatur der Sicherheitsziele nach ISO 27001: Ziel 5.1: Informationssicherheitspolitik
Zweck	Behandlung der für den Datenschutz erforderlichen organisatorischen und technischen Maßnahmen.
Anwendungsgebiet	Alle Aktivitäten von VPrint
Änderungsverlauf	24.10.2017: Entwurfsversion 02.11.2017: endgültige Version

Verfasst durch:	Alain Houbaille
Überprüft durch:	Guillaume Serant
Genehmigt durch:	Thierry Ngoma

Inhaltsverzeichnis

1 Datenschutzverwaltung

2.1 Strategische Norm

Dieses Dokument behandelt die Datenschutzverwaltung, die innerhalb von VPRINT Anwendung findet. Dieses Hauptdokument interagiert mit mehreren anderen Richtlinien und Verfahren, deren wesentlicher Bestandteil es ist.
Zur Erinnerung: Die Kommission für den Schutz der Privatsphäre misst dieser Zielsetzung im Rahmen der persönlichen Datensicherheit große Bedeutung bei.

2.2 Strategische Implikation

Die Information ist eine Ressource, die nach dem Muster anderer wichtiger Produktionsmittel einen erheblichen Wert darstellt, der auf angemessene Weise zu schützen ist. Die Information kann in verschiedenen Formen bestehen. Ungeachtet der Form, die die Information annimmt, und ungeachtet des Mittels zum Teilen, Speichern oder Kommunizieren, muss sie stets auf angemessene Weise geschützt werden.
Darüber hinaus impliziert die neue europäische Richtlinie betreffend den Schutz personenbezogener Daten die Anwendung des Verantwortlichkeitsprinzips und die Verpflichtung des für die Verarbeitung Verantwortlichen, ihre Konformität durch Anwendung einer internen Politik und von Mechanismen, die diese Konformität sicherstellen sollen, nachzuweisen.

VPRINT hat zwecks Beherrschung der mit ihrem Informationssystem verbundenen Risiken und im Bewusstsein der damit einhergehenden Fragen entschieden:

- einen globalen und kohärenten Ansatz zum Schutz ihres Informationsvermögens anzuwenden;
- eine wirksame und ständig verbesserte Sicherheit der von VPRINT im Rahmen ihrer Aktivitäten gespeicherten, verarbeiteten und produzierten Informationen sicherzustellen.

2 Informationssicherheitspolitik

2.1 Kontext

Da der Schutz personenbezogener Daten ein fundamentales Recht ist, dass diese Informationen für das Unternehmen ein strategisches Gut sind, sollte daher darauf geachtet werden, dass die europäische Datenschutzverordnung rigoros eingehalten wird. Da VPRINT personenbezogene Daten verarbeitet, die von ihren Kunden stammen, muss sie über eine Strategie für Informationssicherheit und den Schutz der Privatsphäre verfügen. Diese Strategie ist in diesem Dokument festgelegt. Diese Informationssicherheitspolitik dient somit als Bezugsrahmen zur Realisierung eines Informationssicherheitsmanagements als ein völlig von VPRINT getrennter Prozess.

2.2 Ziele der Informationssicherheitspolitik

Die Informationssicherheitspolitik bildet die Grundlage zur Gewährleistung des Informationsschutzes unter der Verantwortung von VPRINT sowie der Einhaltung der geltenden Gesetze in Bezug auf Informationsverarbeitung und -austausch.

Genauer gesagt, werden folgende Ziele angestrebt:

1. Schutz der Privatsphäre und der gesetzlichen Verpflichtungen betreffend die Verarbeitung von personenbezogenen Daten,
2. die Konformität mit einem Bündel von Sicherheitsmaßnahmen, die im Rahmen der Verarbeitung der vorgenannten Daten anzuwenden sind,
3. die Integration der Informationssicherheit in die Kultur des Unternehmens,
4. die Integration der Sicherheitsanforderungen, die in den Vereinbarungen zwischen dem Unternehmen und Subunternehmern oder externen Stellen festgelegt sind, die mit der Verarbeitung von personenbezogenen Daten zu tun haben,
5. die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen,
6. die ständige Verbesserung der Informationssicherheit bis zu einem gewünschten Grad der Ausreifung.

Diese Politik wird in besondere (untergeordnete) politische Schritte und in Richtlinien umgesetzt, um die sich daraus ergebenden Verpflichtungen zu präzisieren.

2.3 Einhaltung der Politik

Diese Politik ist Bestandteil einer proaktiven Perspektive. Das Erreichen eines optimalen Grads der Informationssicherheit erfordert auf allen Seiten die Verfolgung einer Vision und ein gemeinsames Verständnis der Informationssicherheit und muss sich auf das beständige Engagement von VPRINT, ihrer Mitarbeiter und Subunternehmer stützen. Die Verantwortlichkeit für die Informationssicherheit basiert auf einem kollektiven und individuellen Engagement für:

- den Schutz der zur Verfügung gestellten Informationen, indem diese mit Unterscheidungsvermögen und ausschließlich für die vorgesehenen Zwecke verwendet werden;
- den Schutz sämtlicher Mittel, Vermögenswerte und Orte, von denen aus der Zugriff auf diese Informationen möglich ist.

Der für den täglichen Ablauf Verantwortliche ist für die Anwendung der vorliegenden Politik verantwortlich.

Die Geschäftsleitung von VPRINT besteht auf der Bedeutung der Informationssicherheit innerhalb der Institution und der Verpflichtung sämtlicher Mitarbeiter, sich den Erfordernissen der vorliegenden Politik anzupassen.

Infolgedessen verlangt VPRINT von jeder Person, die ihre Vermögenswerte[1] (z.B. das Informationssystem) benutzt oder die Zugriff auf ihre Informationen hat, sich an die Bestimmungen der vorliegenden Politik sowie an die damit verbundenen Politikschritte, Verfahren und Standards zu halten. Fehler oder unwillentliche Verstöße sind dabei in keinem Fall strafbar. Administrative Maßnahmen sind jedoch denkbar für den Fall, dass vorsätzliche oder wiederholte Verletzungen der Sicherheitsregeln festgestellt wurden.

2.4 Geltungsbereich

Die vorliegende Informationssicherheitspolitik sowie die zugrunde liegenden Richtlinien und Verfahren und die damit einhergehenden Regeln gelten für die nachstehenden Personen, Vermögenswerte und Aktivitäten:

- Für das gesamte Personal von VPRINT, sowohl internes als auch externes Personal, und zwar einschließlich des Leihpersonals, sowohl befristet als auch unbefristet (z.B. Berater, Lieferanten, Praktikanten, Aushilfskräfte usw.).
- Für jede natürliche oder juristische Person, die – sei es für Rechnung der Organisation oder nicht – vertrauliche oder nicht vertrauliche Informationen benutzt oder darauf zugreift.
- Für sämtliche Vermögenswerte sowie deren Einsatz innerhalb der Organisation, wie zum Beispiel elektronische Datenbanken, Informationen, ungeachtet des Trägermediums, Kommunikationsnetze, Informationssysteme, Software oder Datenverarbeitungszentren.
- Für sämtliche Aktivitäten zum Austausch personenbezogener Daten zwischen den Informationssystemen von VPRINT und den anerkannten externen Stellen.

2.5 Anwendung und Weiterentwicklungen

Die Validierung der vorliegenden Datenschutzverwaltung durch den für das tägliche Management Verantwortlichen bei VPRINT oder durch den Vorstand verleiht ihr Anwendbarkeitscharakter. In diesem Rahmen verpflichtet sich die Geschäftsleitung zur Bereitstellung der notwendigen

[1] Als Vermögenswert gilt jedes Element, welches für die Organisation einen Wert hat und infolgedessen einen ausreichenden Schutz bedingt (ISO-Norm 27005, 8.2.1.2).

Ressourcen und zur periodischen Neubewertung dieser Politik, um so neue Bedürfnisse, neue Methoden und Technologien, neue Bedrohungen und auftretende Risiken zu berücksichtigen. Jede Änderung der vorliegenden Politik bedarf der Billigung durch den Vorstand.

3 Organisatorische und technische Maßnahmen

Das Bezugssystem von organisatorischen und technischen Maßnahmen, die für den Datenschutz bei VPRINT angewandt werden, basiert auf der Norm "ISO 27001: 2013 – Leitfaden für das Management der Informationssicherheit" und den Referenzmaßnahmen des BDSG[2]. Diese Maßnahmen sind nachstehend aufgeführt:

3.1 Organisation der Sicherheit (ISO 27001, Abschnitt 6)

3.1.1 Organisation

- VPRINT hat einen Sicherheitsreferenten eingesetzt, der auch für den Datenschutz zuständig ist.
- Der Sicherheitsreferent spielt eine koordinierende Rolle bei der Umsetzung und Anwendung der Datenschutzverwaltung. Er tritt als Sicherheitsleiter für das gesamte neue Projekt auf, koordiniert den täglichen Ablauf der Funktion als Datenschutzbeauftragter (DPO), ist an der Homogenisierung des Sicherheitsniveaus beteiligt und hält sich über den aktuellen Stand im Bereich TIC (Informations- und Kommunikationstechnologie) auf dem Laufenden und kontrolliert die Einhaltung der gesetzlichen Anforderungen, darunter der Schutz personenbezogener Daten.

3.1.2 Mobilgeräte und Homeoffice

- Homeoffice oder Fernwartung sind Gegenstand von Vorrichtungen und Verfahren zur Fernzugriffs- und Verschlüsselungskontrolle.
- Der wesentliche Teil der Homeoffice-Arbeit findet nur über ein virtuelles Büro statt, wodurch die Informationsverarbeitung und -speicherung mit privater Ausrüstung verhindert wird.

3.2 Sicherheit der Personalressourcen (ISO 27001, Abschnitt 7)

- Jeder (interne und externe) Mitarbeiter von VPRINT unterzeichnet bei seiner Einstellung eine Geheimhaltungsverpflichtung.
- Das (interne oder externe) Personal erhält regelmäßig eine Erinnerung an die Verpflichtungen zur Wahrung des Berufsgeheimnisses und an die Geheimhaltungsklauseln.
- Eine Benutzersatzung mit den allgemeinen Begrenzungen der Benutzung der VPRINT-Informationssysteme, der Rechte und Pflichten der Benutzer, der durch den Sicherheitsreferenten ausgeführten Kontrollen und der Konsequenzen im Fall einer

[2] BDSG: Bundesdatenschutzgesetz – deutsches Gesetz für den Datenschutz.

Verletzung der Regeln wird jedem Benutzer bei seiner Ankunft ausgehändigt. Dieses Dokument wird jedem neuen Arbeitnehmer zur Kenntnis gebracht, ganz gleich, ob er auf Zeit, fest oder als externer Mitarbeiter eingestellt wird.

- Sitzungen zur Sensibilisierung in Bezug auf die Sicherheit und die neue europäische Datenschutzgesetzgebung finden regelmäßig statt, die Benutzer werden hinsichtlich ihrer Verantwortlichkeiten und der richtigen Sicherheitsmethoden für den Datenschutz sensibilisiert.

3.3 Verwaltung der Vermögenswerte (ISO 27001, Abschnitt 8)

- Alle "Berufsdienstleistungen" sind in speziellen Verzeichnissen aufgeführt, einschließlich der verwendeten Software und Server.
- Ein Tätigkeitsregister für sämtliche Verarbeitungsvorgänge mit personenbezogenen Daten, die VPRINT durchführt, wird eingerichtet und aktualisiert.
- Ein Bündel von Verfahren betreffend die Manipulation personenbezogener Daten wird dokumentiert und eingerichtet. Diese Verfahren decken den gesamten Lebenszyklus der vorgenannten Informationen ab, und zwar: Erstellung, Verarbeitung, Übertragung, Speicherung, Sicherung, Archivierung und Vernichtung (z.B. geschützte Entsorgung von Datenträgern oder Papierunterlagen).

3.4 Logische Zugangsberechtigung (ISO 27001, Abschnitt 9)

- Die Identifizierung der sich in das Netz einwählenden Person erfolgt eindeutig und unverwechselbar. Sämtliche Benutzer der Informationssysteme (interne Benutzer, Drittbenutzer usw.) besitzen ein Namenskonto.
- Jede Erstellung, Änderung oder Schließung eines Kontos (Benutzer, Administrator, Dienst usw.) wird durch den Sicherheitsreferenten überwacht und verfolgt.
- Sämtliche Zugriffe auf Informationssysteme werden rückverfolgt.
- Benutzer mit hohen Zugriffsrechten werden in einem Bezugssystem (Namenskonten und Dienstkonten) erfasst.
- Das Verfahren der Bewegungen (Eingang, Ausgang oder interne Veränderung) wird erfasst und schließt die Aktualisierung des Bezugssystems und der damit einhergehenden Zugriffsrechte ein. Es berücksichtigt Profil und Dauer der Aufgabenstellung des neuen Benutzers (interner Benutzer oder Drittbenutzer).
- Eine Politik komplexer Passwörter für den Zugriff sämtlicher Benutzer der SI (interne Benutzer, Drittbenutzer) und der Dienstkonten wird festgelegt, die die Empfehlungen bezüglich der Sicherheit einhalten: Komplexität, Mindestlänge, Begrenzung von Zugriffsversuchen usw.
- Es werden Vorrichtungen zur zeitlichen Begrenzung der Zugangsberechtigungen eingerichtet, um den Schutz des Zugriffs auf die Informationssysteme sicherzustellen: aktivierter und durch Passwort geschützter Bildschirmschoner, Deaktivierung der Sitzung

am Ende des Tages usw.

3.5 Physische und Umweltsicherheit (ISO 27001, Abschnitt 11)

3.5.1 Gesicherte Zonen

- Die Sicherheitsbereiche sind eindeutig festgelegt. Die gesicherten Zonen sind gegen jeden Zugriffsversuch durch gewaltsames Eindringen geschützt und mit einer progressiven physischen Zugriffsschutzvorrichtung ausgestattet (Ebenen und Abschirmung), die an die Art der mit dem Verkehr von "unbefugten" Personen verbundenen Risiken angepasst ist.
- Der Zugang zu technischen und sensiblen Räumen ist namensgebunden und ist nur Personen gestattet, die vom Sicherheitsreferenten entsprechend befugt wurden. Die berechtigten Personen werden registriert und die Zugriffe protokolliert.
- Das interne Personal von VPRINT und die Lieferanten müssen alleine aufgrund des Prinzips des "Kenntnisbedarfs" über das Bestehen gesicherter Zonen innerhalb der die VPRINT-Vermögenswerte beherbergenden Gebäude informiert werden.
- Die nicht belegten gesicherten Zonen müssen gesperrt und in periodischen Abständen kontrolliert werden.
- Alle Foto-, Videogeräte und sonstigen Aufzeichnungsvorrichtungen, wie in mobile Geräte integrierte Fotoapparate, sind in den gesicherten Zonen verboten, sofern keine gegenteilige Genehmigung erteilt wurde.
- Nur Personen, die registriert oder in einem Besuchsregister eingetragen sind, haben Zutritt zum Gelände. Die Besucher erhalten eine Plakette, mit der sie beim Betreten des Geländes identifiziert werden können.
- Drittbeteiligte, die nicht vertraglich befugt sind, und Besucher werden von einer befugten Person begleitet.
- Die Liste der berechtigten Personen wird vom Sicherheitsreferenten regelmäßig überprüft.

3.5.2 Material

- Nicht entmaterialisierte Elemente, wie Archive, Fertigprodukte, werden in dafür geeigneten Räumen gelagert, um sie gegen Diebstahl und Umweltgefahren zu schützen.
- Alle Informatikeinrichtungen, die als für VPRINT wichtig oder existenziell erfasst sind, werden in gesicherten Räumlichkeiten, bezeichnet als Informatikraum oder Technikräume, installiert.
- Der Schutz sensibler Ausrüstungen erfolgt durch Präventions- und/oder Schutzmaßnahmen entsprechend dem Grad ihrer Sensibilität (Brandschutz, Klimatisierung, elektrische Hilfseinheiten (UPS)).
- Sensibles Material (Server, Netzausrüstungen) ist gegen Stromversorgungsstörungen (zum Beispiel Überspannung) geschützt und verfügt über eine Notstromversorgung, womit die Verfügbarkeit der erwarteten Leistung garantiert werden kann.
- Für als sensibel eingestufte Vermögenswerte wird ein Wartungsvertrag mit garantierter Einsatz- oder Austauschzeit geschlossen, der die Verfügbarkeits- und

Vollständigkeitsanforderungen des Vermögenswerts erfüllt.

- Speicherträger, die vertrauliche Informationen enthalten, werden physisch zerstört; dadurch werden sie endgültig unbrauchbar gemacht.
- Die Entsorgung von Papier, welches personenbezogene Daten enthält, erfolgt durch eine für die Vernichtung von Papier zugelassene Spezialfirma.
- Die Politik eines ordentlichen Büros und eines leeren Bildschirms ist dem Personal bekannt und findet bei VPRINT Anwendung, damit keinerlei sensible Informationen unbewacht zurückbleiben.

3.6 Sicherheit in Verbindung mit dem Betrieb (ISO 27001, Abschnitt 12)

3.6.1 Schutz gegen Schadsoftware

- Alle Server und Arbeitsplätze sind geschützt und werden überwacht, um die Unversehrtheit der Informationen (Daten, Konfiguration usw.) zu gewährleisten.
- Die Internetverbindungen der Benutzer werden gefiltert und protokolliert. Eine Liste der nicht zugelassenen Plätze wird von dem für diese Aspekte zuständigen Referenten erstellt und regelmäßig aktualisiert.

3.6.2 Datensicherung

- Eine Datensicherungspolitik wird von dem für diese Aspekte zuständigen Sicherheitsreferenten formalisiert und validiert. Sie berücksichtigt: den Datenschutzbeauftragten, Häufigkeit, Typ (komplett, inkrementell, differenziell), Trägermaterial, Verwahrungsfrist, regelmäßige Wiederherstellungstests und die Kontrolle der Unversehrtheit der gesicherten Daten.

3.6.3 Protokollierung und Überwachung

- Die Spurenerfassung wird innerhalb der Infrastruktur der VPRINT-Informationssysteme sichergestellt, um zwei Zwecke zu erreichen:
  - die "Einhaltung der Gesetze betreffend die Privatsphäre";
  - die Erkennung von Sicherheitsverletzungen und -zwischenfällen.
- Eine Richtlinie zur Anwendung der Spurenerfassung adressiert die Spezifikationen in Bezug auf Inhalt, Schutz und Verwahrung der Spuren.

3.6.4 Kontrolle der Betriebssoftware

- Die Mitarbeiter von VPRINT sind nicht berechtigt, auf in Betrieb befindlichen Systemen Software zu installieren. Die Installation oder Aktualisierung von Software während des Betriebs darf nur durch qualifizierte Administratoren erfolgen.
- Die Standardisierung der Konfiguration der Betriebssysteme garantiert das angemessene

Sicherheitsniveau.

3.6.5 Umgang mit technischen Verwundbarkeiten

- Ein formeller Prozess für den Umgang mit technischen Verwundbarkeiten ist definiert und eingerichtet. Dieser Prozess hängt mit der Verwaltung der Vermögenswerte zusammen und umfasst insbesondere die Überwachung in Bezug auf Verwundbarkeit, Risikobewertung, Anwendung von Software-Korrektiven und Verfolgung der Aktionen.

3.7 Kommunikationssicherheit (ISO 27001, Abschnitt 13)

3.7.1 Management der Netzsicherheit

- Die Architektur des Netzes garantiert die logische Abschirmung zwischen den verschiedenen Vertrauensbereichen.
- Filter-, Umschalt- und Routereinrichtungen sind so konfiguriert, dass die Beförderung nur der autorisierten Datenströme an diejenigen Empfänger garantiert ist, die sie erhalten sollen.
- Die autorisierten Datenströme und Protokolle werden entsprechend ihrer unverzichtbaren Beschaffenheit rigoros ausgewählt und regelmäßig kontrolliert.
- Alle durch Netzeinrichtungen (Brandschutz) entdeckten Unregelmäßigkeiten und die festgelegten Sitzungsmerkmale werden zu Auditzwecken registriert und archiviert.
- Verfahren zur Wartung der Netzeinrichtungen sind definiert und finden Anwendung.
- Netzschaltpläne, Bestandsdokument (Material- und Softwareliste) und Konfigurationselemente (Adressierungsplan, Router- und Filterregeln usw.) werden dokumentiert und regelmäßig aktualisiert.

3.7.2 Informationsübertragung

- Es bestehen eine formelle Übertragungspolitik und formelle Übertragungsmaßnahmen zum Schutz sensibler Informationen (personenbezogene Daten), die über ein externes Informatiknetz laufen.
- Ausdrückliche Vereinbarungen in Verbindung mit der gesicherten Übertragung von sensiblen Informationen werden zwischen VPRINT und den Drittbeteiligten systematisch angefordert.

3.8 Untervergabe (ISO 27001, Abschnitt 15)

- Mit den Dienstleistern geschlossene Vereinbarungen schließen eine Geheimhaltungsverpflichtung ein.
- In den mit den Lieferanten getroffenen Vereinbarungen ist festgelegt, dass sie die

notwendigen Vorkehrungen beinhalten, damit Regeln zum Schutz personenbezogener Daten eingehalten werden.

- Je nach Umfang der angeforderten Dienstleistung sind folgende Sicherheitsanforderungen in die Untervergabeverträge integriert:
  - die Verantwortlichkeiten in Bezug auf Sicherheit für VPRINT und für den Subunternehmer;
  - die Überprüfung der Einhaltung der Geheimhaltungs- und Integritätsanforderungen der Informationen;
  - die Maßnahmen zur Kontrolle des physischen und logischen Zugriffs, die vorzusehen und einzuhalten sind;
  - die Kontinuitätsmessungen des Betriebs in einem Schadensfall;
  - die Ebene des physischen Schutzes von Material, welches Dritten anvertraut ist;
  - das Recht zur Prüfung der Anwendung, Verfahren und Sicherheitsanlagen.

3.9 Umgang mit Sicherheitszwischenfällen (ISO 27001, Abschnitt 16)

- Im Fall einer Infektion (Wurm, Virus, Trojaner), einer Sicherheitslücke oder jeder Datenverletzung, die an einem Arbeitsplatz festgestellt oder vermutet werden, wird ein Reaktionsverfahren eingerichtet, welches sämtlichen Nutzern und Lieferanten bekannt ist.
- Es wird ein Zwischenfallregister auf dem neuesten Stand gehalten, welches es erlaubt, Zwischenfälle, Ursprung, Ursache, Auswirkung auf die Verfügbarkeit, Integrität oder Verlässlichkeit sowie ergriffene Maßnahmen zahlenmäßig zu erfassen.
- Jede Verletzung von personenbezogenen Daten wird gemäß einem formellen Verfahren evaluiert und zurückverfolgt.

3.10 Kontinuitätsverwaltung (ISO 27001, Abschnitt 17)

- In Übereinstimmung mit den Branchenzielen der Organisation wurden ein Informatik-Notfallplan und ein Aktivitätskontinuitätsplan erstellt, um bei einem Notlauf einen Mindestbetrieb sicherzustellen.
- Die Informatik-Notfallverfahren und -Lösungen werden regelmäßig durch das Informatikteam getestet.

3.11 Konformität (ISO 27001, Abschnitt 18)

- Die Geschäftsleitung von VPRINT muss sich von der Konformität der Datenverarbeitung

und der Verfahren, für die sie zuständig ist, im Hinblick auf die anwendbare Sicherheitspolitik, die Gesetze und die geltenden Vorschriften überzeugen.

- In periodischen Abständen muss die technische Sicherheit des Informationssystems überprüft werden, um zu gewährleisten, dass die Material- und Software-Sicherheitskontrollen korrekt angewandt wurden. Diese technische Sicherheitsprüfung schließt insbesondere Einbruchstests und die Bewertung der Verwundbarkeiten der Informationssysteme ein, die der Verantwortlichkeit von VPRINT unterliegen, einschließlich derjenigen, die von Dritten auf Rechnung von VPRINT abgewickelt werden.