IT-Richtlinie
für den Flughafen Basel-Mulhouse
Richtlinie für die Nutzung der neuen Informations- und Kommunikationstechnologien

Vorbemerkung

Der Flughafen Basel-Mulhouse, genauer die IT-Abteilung hat ein Informations- und Kommunikationssystem eingerichtet, das insbesondere ein Computernetz umfasst, welches für seinen Geschäftsbetrieb notwendig ist.

Zur Erfüllung ihrer Aufgaben müssen die Mitarbeiter auf das Informations- und Kommunikationssystem, das ihnen zur Verfügung gestellt wird, zugreifen und dieses benutzen.

Das Informations- und Kommunikationssystem des Flughafens ist jedoch ständig erheblichen Risiken ausgesetzt, die seine technische Integrität bedrohen (Viren, Ausfälle).

Deshalb wurden mit dieser IT-Richtlinie Regeln für die Nutzung der IT-Ressourcen aufgestellt, zu deren Einhaltung sich jeder Nutzer verpflichtet.

Die Flughafen-Mitarbeiter müssen außerdem verantwortungsbewusst handeln und zur Sicherheit des im Flughafen bereitgestellten Systems beitragen.

Daher informiert die IT-Richtlinie die Mitarbeiter des Flughafens über die guten Praktiken bei der Nutzung der bereitgestellten IT-Ressourcen und die einzuhaltenden Sicherheitsregeln sowie die vom Flughafen getroffenen Schutzvorkehrungen.

Alle diese Bestimmungen tragen zum reibungslosen Funktionieren des Informations- und Kommunikationssystems und zum Schutz des Rufes des Flughafens bei.

Anwendungsbereich der IT-Richtlinie

Die Richtlinie gilt für alle Mitarbeiter des Flughafens, welche die Hardware und die Software nutzen, die das Informations- und Kommunikationssystem des Flughafens bilden.

Sie gilt auch für alle anderen Personen, die auf dem Flughafen tätig sind und die Hard- und Software des Informations- und Kommunikationssystems des Flughafens benutzen, unabhängig von der Art und der Dauer ihres Einsatzes (wie etwa Mitarbeiter externer Unternehmen und Subunternehmer, die auf dem Flughafen tätig sind, Beamte und gleichgestellte Bedienstete der öffentlichen Behörden, Zeitarbeitnehmer, Praktikanten).

Das Informations- und Kommunikationssystem des Flughafens umfasst folgende Bestandteile: stationäre und tragbare Rechner, Tablets, Smartphones, Telefone, Server, Software, Dateien, Daten, Datenbanken und Mitteilungssystem.

INHALT

I. Rechtlicher Rahmen

Der Flughafen und die PSSIE	• Jeder Mitarbeiter ist an die Richtlinie des französischen Staates für die Sicherheit der Informationssysteme (Politique de Sécurité des Systèmes d'Information de l'Etat Français, PSSIE) gebunden. • Die PSSIE enthält konkrete Anforderungen, auf die diese Richtlinie Bezug nimmt.
Pflichten der Flughafen-Mitarbeiter	• Die Mitarbeiter müssen die IT-Werkzeuge und IT-Ressourcen für die Zwecke ihrer beruflichen Tätigkeit verwenden. • Eine ausnahmsweise Nutzung für private Zwecke kann jedoch von den jeweiligen Abteilungsleitern geduldet werden, doch darf eine solche Nutzung in keinem Fall die Tätigkeit des Mitarbeiters und die Erfüllung der ihm übertragenen Aufgaben behindern oder beeinträchtigen. Laut Gesetz kann der Mitarbeiter zivil- und/oder strafrechtlich zur Verantwortung gezogen werden, wenn er für private Zwecke eine Internetseite besucht, die gegen geltende Vorschriften und die guten Sitten verstößt. Daher behält es sich die Führungsebene vor, jegliche Internetnutzung für private Zwecke zu verbieten, wenn diese ein Risiko für den ungestörten Flughafenbetrieb darstellt. • Jeder Mitarbeiter verpflichtet sich, die Bestimmungen dieser Richtlinie einzuhalten. Anderenfalls können die nach der Betriebsordnung vorgesehenen Strafen gegen den Mitarbeiter verhängt werden.
Einsichtsrecht des Flughafens	• Die Unterlagen und Dokumente, die von den Mitarbeitern erstellt wurden und im Netzwerk des Flughafens gespeichert sind, werden als geschäftlich angesehen, soweit nichts anderes vermerkt ist. • Um seine Sicherheit und sein Ansehen zu schützen, behält es sich der Flughafen vor, die Verkehrsdaten (Daten, die im Netz und im Internet fließen) sowie die gespeicherten Unterlagen und Dokumente unter Einhaltung der geltenden Gesetze zu analysieren. • Was die Daten privater Natur betrifft, ist es Sache des Arbeitnehmers, diese gegebenenfalls in ausdrücklich hierfür vorgesehene Dateien mit der Bezeichnung *„Persönlich"* oder *„Privat"* abzulegen. Der Schutz und die regelmäßige Sicherung dieser Daten sind Aufgabe des Mitarbeiters. • Der Flughafen kann in die als *„Persönlich"* oder *„Privat"* gekennzeichneten Dateien in Gegenwart des Mitarbeiters oder eines Personalvertreters Einsicht nehmen, jedoch nur unter der Voraussetzung, dass der Mitarbeiter vorher ordnungsgemäß informiert wurde. • Der Zugang zu Informationen, die in Ereignisprotokolldateien (Logsystemen) enthalten sind, ist den Systemadministratoren

	vorbehalten, die sich zur Einhaltung der Aministratoren-Richtlinie verpflichten. Die Speicherfrist der Ereignisprotokolldateien mit direktem oder indirektem Namensbezug beträgt ein Jahr. • Die Frist kann länger sein, wenn eine Datei dazu bestimmt ist, als Beweis im Rahmen der Beilegung eines Streits oder bei der Klärung einer Zuwiderhandlung herangezogen zu werden.
Kontrollrecht des Flughafens	• Die Flughafenleitung behält es sich vor, die Einhaltung dieser Richtlinie zu kontrollieren. • Die Kontrolle erfolgt in der für die IT-Systeme zuständigen Abteilung durch namentlich benannte Personen. Sie kann insbesondere eine Aufstellung der Dauer der Internetverbindung, eine Aufstellung der besuchten Webseiten, eine Analyse des Formats und der Größe der erhaltenen oder versandten Dateianhänge umfassen.
Sanktionsrecht des Flughafens	• Bei Nichteinhaltung der in dieser Richtlinie festgelegten Sicherheitsregeln und -maßnahmen wird der Nutzer persönlich zur Verantwortung gezogen, sofern bewiesen ist, dass er die schuldhaften Handlungen persönlich zu vertreten hat. Folglich können den begangenen Verstößen angemessenen Disziplinarstrafen, die in der Betriebsordnung festgelegt sind, gegen ihn verhängt werden.

II. Information und Mitwirkung der Mitarbeiter

Einsichtnahme in die Richtlinie	<u>Die Richtlinie kann abgerufen werden:</u> • von benannten Windows-Anwendern und Praktikanten (Bsp. „stageit“) bei der Anmeldung in Windows • von allen gewöhnlichen Windows-Anwendern über die Intranet-Seite.
Annahme der Richtlinie	• Für benannte Windows-Anwender und Praktikanten (Bsp. „stageit“) erfolgt die Annahme durch elektronische Bestätigung bei der Anmeldung in Windows. • Für gewöhnliche Windows-Anwender (Bsp.: „serviceaccueil“) erfolgt die Annahme durch Unterzeichnung des vom Verantwortlichen für Informationssicherheit (Chief Information Security Officer, CISO) zugeschickten gedruckten Dokuments und Rücksendung des unterschriebenen Dokuments an den CISO.
Beitrag zum Schutz des Ansehens und zur IT-Sicherheit des Flughafens	• Mit Zustimmung seiner Vorgesetzten kann jeder Mitarbeiter sich zu einer Sensibilisierungsveranstaltung anmelden, die von der IT-Abteilung organisiert wird. • Jeder Mitarbeiter hat den Koordinationszentrum jeden Sachverhalt zu melden, der von der IT-Richtlinie abweicht und/oder den Schutz personenbezogener Daten betrifft.

III. Erlaubte und verbotene Hard- und Software

Erlaubte IT-Ausstattung	• Die Mitarbeiter des Flughafens haben **ausschließlich** Hardware-Ausstattung (wie etwa stationäre und tragbare Rechner, Tablets, Smartphones, Telefone) sowie die Server und Softwareprogramme, die unter der Verantwortung der IT-Abteilung bereitgestellt und konfiguriert wurden, die Dateisysteme, Daten und Datenbanken, sowie das Mitteilungssystem zu benutzen. Der Anschluss eines Modems oder ein direkter Internetanschluss über einen Internetdienstanbieter sind streng **verboten**. • Die vom Flughafen bereitgestellte Ausstattung (Anschluss oder Objektspeicher) ist für den beruflichen Gebrauch bestimmt; eine ausnahmsweise Nutzung für private Zwecke wird gleichwohl geduldet. • Wenn nötig, erlaubt der Flughafen dem Mitarbeiter die Nutzung des Laufwerks D: seines Rechners zur Speicherung von privaten Dateien (Es ist zu beachten, dass Daten, die auf den Laufwerken C: und D: abgelegt sind, vom Flughafen nicht gesichert werden.). • Die Mitarbeiter müssen die Netzlaufwerke (also nicht D:) für die Speicherung geschäftlicher Daten benutzen. Hinweise zur Nutzung: - *„Persönlich/Öffentlich“*: Persönliche geschäftliche Dokumente im gemeinsamen Lesezugriff - *„Persönlich/Privat“*: Persönliche geschäftliche Dokumente ohne gemeinsamen Lesezugriff • Die Mitarbeiter dürfen nur solche externen Speichermedien (USB-Stick, externe Festplatte, SD-Karte etc.) benutzen, die ausschließlich geschäftlichen Zwecken dienen und deren Herkunft geklärt ist. • Die Zuteilung der Hard- und Software erfolgt im Rahmen des *„Verfahrens zur Zuteilung von IT-Ressourcen und Abschlussverfahren“*, falls erforderlich nach besonderer Anforderung über das Koordinationszentrum. • Die Mitarbeiter müssen mit der zugeteilten Hard- und Software sorgfältig umgehen.
Verbotene IT-Ausstattung	• Die Verbindung mit dem Flughafennetzwerk AÉROPORT (außer über den Hotspot „Guest“) mit Hilfe von Hardware und/oder Software, die nicht von der IT-Abteilung bereitgestellt und konfiguriert wurde, ist **verboten**. • Bei Bedarf müssen die Mitarbeiter ihre Bitte um Befreiung von diesem Verbot an das Koordinationszentrum richten. • Die Mitarbeiter dürfen die Konfiguration einer bereitgestellten Hardware oder Software nicht absichtlich ändern. • Bei Funktionsstörungen müssen sich die Mitarbeiter an den Koordinationszentrum wenden.

IV. Verwaltung der Zugriffsrechte für die Anwendungen

Zugriffsrechte für die Anwendungen	• Die Zugriffsrechte für die Anwendungen werden von den Verantwortlichen für den Anwendungsbereich verwaltet, die in dem im Qualitätssystem verfügbaren Verzeichnis genannt sind.

V. Beitrag zur Sicherheit

Rechte entsprechend dem Aufgabengebiet des Mitarbeiters	• Aus Sicherheitsgründen werden die Zugriffsrechte für externe Anwendungsressourcen (z.B. Webseiten) und interne Anwendungsressourcen (z.B. Server, Dateibäume) anfänglich festgelegt und dann an das Aufgabengebiet des Mitarbeiters angepasst. • Falls eine Änderung dieser Zugriffsrechte notwendig sein sollte, muss der Mitarbeiter seine Anfrage, die vorab von seinen Vorgesetzten freizugeben ist, an das Koordinationszentrum richten. • Der Zugang zu diesen Ressourcen kann bei der Beendigung der beruflichen Tätigkeit des Mitarbeiters entzogen werden, auch wenn die Beendigung nur vorläufig erfolgt. • Jeder Mitarbeiter hat ein Recht auf Abschalten, das durch einer einseitigen Richtlinie zum Recht auf Abschalten vom 11. Januar 2018 geregelt ist.
Keine Vergabe von Administratorrechten	• Aus Sicherheitsgründen liegen die Administratorrechte für die Hardware ausschließlich bei der IT-Abteilung. • Bei mutmaßlichen oder erwiesenen Funktionsstörungen muss der Mitarbeiter sich mit dem Koordinationszentrum in Verbindung setzen.
Benutzerkennungen und Passwörter nicht sichtbar	• Jeder ist für die Verwendung seiner Passwörter selbst verantwortlich. Für die Nutzung geschützter Anwendungen, die nur mit Passwort zugänglich sind, ist der Inhaber des Passworts verantwortlich, es sei denn, dass eine missbräuchliche Nutzung durch einen Dritten nachgewiesen wurde. • Die Mitarbeiter müssen Passwörter wählen, die nicht trivial sind und das gegebenenfalls von der IT-Abteilung vorgeschriebene Format einhalten. • Es wird den Mitarbeiter empfohlen, ihre Passwörter regelmäßig zu ändern und sie streng geheim zu halten. • Bei dienstlicher Notwendigkeit kann ein weiterer Mitarbeiter Zugang zu dem Nachrichtenpostfach eines Nutzers durch entsprechende Parametrierung der Postfächer erhalten, so dass eine Weitergabe von Passwörtern vermieden wird.
Notwendigkeit der Sperrung der Geräte	• Die Mitarbeiter müssen ihren Computer sperren (auf Standby setzen mit Passwortanforderung), wenn sie ihren Arbeitsplatz

	verlassen oder wenn der Computer außerhalb ihrer Sichtweite ist.
Zugang für Dritte	• Die Mitarbeiter dürfen unbefugten Nutzern keinen Zugang zu den Systemen oder Netzen des Flughafens verschaffen. • Der Zugang eines Nutzers zu den Informationen und Dokumenten, die in den IT-Systemen und Computernetzen gespeichert sind, ist auf seine eigenen, auf öffentliche oder aber auf gemeinsam genutzte Informationen und Dokumente beschränkt. Folglich darf niemand jemals versuchen, auf Daten oder Informationen (Nachrichten, Dateien etc.), die einem Anderen gehören, ohne dessen vorherige Zustimmung zuzugreifen, solche Daten oder Informationen zu kopieren, zu ändern oder zu vernichten.
Wachsamkeit	• Jeder Mitarbeiter muss das Koordinationszentrum unverzüglich jeden versuchten unberechtigten Zugriff auf sein Benutzerkonto oder seine persönlichen Daten sowie jede Funktionsstörung melden.
Nutzung einer neuen Anwendung	• Jeder Mitarbeiter muss sich an das Dokument „Empfehlungen zur IT“ halten, das im Qualitätssystem verfügbar ist. Bei Schwierigkeiten muss er sich an den IT-Verantwortlichen wenden.
Pflichten jedes Mitarbeiters bei längerer Abwesenheit oder bei Beendigung der Tätigkeit	• Vor seinem endgültigen Ausscheiden, unabhängig davon, was der Grund dafür ist (Vertragsbeendigung, Auftragsende etc.), ist der Nutzer verpflichtet, - die unter *„Persönlich“*, *„Privat“* abgelegten Verzeichnisse oder Dokumente spätestens am Tag vor seinem Austritt zu löschen. Anderenfalls werden diese Verzeichnisse, sofern nicht ein Gerichtsverfahren oder eine behördlichen Ermittlung läuft, am Tag nach dem Austritt des Nutzers aus dem Flughafenbetrieb automatisch gelöscht, ohne dass diese eingesehen werden und ohne dass eine Kopie erstellt wird. - seinen Vorgesetzten spätestens bei seinem Austritt oder unverzüglich nach erster Anforderung seiner Vorgesetzten die gesamte IT-Ausstattung und alle elektronischen Kommunikationsmittel (Rechner, Mobiltelefon, Zutrittsausweise, Mittel zur Remote-Authentifizierung etc.), die ihm im Rahmen seiner Aufgaben zur Verfügung gestellt wurden, in gutem Betriebszustand zurückzugeben.
Mutwillige Eingriffe in das IT-System	• Es ist ausdrücklich verboten, - die Funktion der bereitgestellten Hardware und Software sowie der IT-Systeme des Flughafens absichtlich zu stören - absichtlich mutwillige Eingriffe jedweder Art in das IT-System zu verüben, gleichgültig, auf welche Weise dies geschieht, insbesondere durch unsachgemäßen Gebrauch der Hardware oder durch unzulässiges Einbringen von Schadsoftware (Netz-

	Ausspähsoftware, Computerviren, Trojanische Pferde, Logikbomben); es drohen bei solchen Eingriffen die in der Betriebsordnung vorgesehenen Disziplinarstrafen.
Gesetzliche Bestimmungen	• Die Mitarbeiter dürfen urheberrechtlich geschützte Daten oder Dateien (MP3, Videos, Spiele, sonstige Software) weder herunterladen noch kopieren, verschicken oder verwenden. • Die Mitarbeiter dürfen nicht auf Webseiten zugreifen, deren Inhalt rechtswidrig ist oder gegen die guten Sitten verstößt.

VI. Austausch mit externen Teilnehmern

Berufsethik	• Generell muss sich jeder Mitarbeiter bei der Nutzung der vom Flughafen bereitgestellten IT-Ressourcen an die geltenden Gesetze und an den Grundsatz der Höflichkeit halten. • Kein Mitarbeiter darf Dokumente oder Mitteilungen verbreiten, die verleumderisch oder beleidigend sind oder ausdrückliche oder versteckte Drohungen enthalten oder zum Mobbing einer Person in irgendeiner Form beitragen. • Kein Mitarbeiter darf Dokumente, Informationen, Bilder oder Videos, die rechtswidrig sind (Pädophilie, Rassismus, Nationalsozialismus, Verherrlichung von Verbrechen oder Gewalt, Terrorismus etc.) oder gegen die guten Sitten verstoßen (Pornografie u.a.) laden, speichern, verbreiten oder verteilen oder zum Versand solcher Dokumente auffordern. • Jeder Mitarbeiter muss das Image und den externen und internen Ruf des Flughafens schützen. • Abgesehen von der Möglichkeit, eine Nachricht aus dienstlichen Gründen über die Verteiler des Flughafens zu verbreiten, darf kein Mitarbeiter Massen-Nachrichten verschicken. • Kein Mitarbeiter darf auf Massennachrichten antworten. • Jeder Mitarbeiter muss es der Koordinationszentrum melden, wenn der Verdacht besteht, dass ein Teil der IT-Ausstattung (z.B. Dateisystem, Arbeitsplatz, externes Speichermedium etc.) von einem Virus befallen ist.
Nach außen weitergegebene Daten	• Um die Offenlegung vertraulicher Informationen zu vermeiden, für die der Flughafen haftbar gemacht werden kann, darf jeder Mitarbeiter nur das notwendige Mindestmaß an Informationen am Empfänger außerhalb des Flughafens übermitteln. Diese Regel gilt unabhängig von der Art der Übermittlung der Information: E-Mail, Austauschplattformen, bewegliche Datenträger etc.
Von außen erhaltene Daten	• Empfangene Daten können Viren enthalten, die den Rechner des Mitarbeiters oder gar das gesamte Flughafennetz infizieren können.

	Für den Datenempfang darf der Mitarbeiter nur Plattformen zum Austausch von Dateien verwenden, die von der IT-Abteilung freigegeben und bereitgestellt wurden. Jeder Mitarbeiter darf nur solche beweglichen Datenträger verwenden, die aus zuverlässigen Quellen stammen. Im Zweifelsfall muss er sich unverzüglich mit den Koordinationszentrum in Verbindung setzen.

VII. Kontaktstelle

Einzuschaltende Koordinations-zentrum (1010)	• Das Koordinationszentrum ist in folgenden Fällen zu benachrichtigen: - wenn ein Mitarbeiter den Verdacht hat, dass sein Rechner infiziert ist, dass er ein ungewöhnlich hohes Berechtigungsniveau (Administrator des Rechners u.a.) oder eingeschränkte Rechte hat, oder wenn eine sonstige Anomalie vorliegt - bei Verlust oder Verdacht auf Diebstahl eines Geräts - im Falle der Notwendigkeit einer Änderung der Rechte für die internen Ressourcen - wenn eine E-Mail von Mailcontrol unter Quarantäne gestellt wurde und sich der Mitarbeiter Gewissheit über ihre Herkunft verschafft hat - wenn er Fragen zur Sicherheit des IT-Systems hat.

VIII. Schutz persönlicher Daten

Schutz persönlicher Daten	• Der Flughafen misst der Achtung der Privatsphäre seiner Mitarbeiter große Bedeutung bei. • Alle Vorgänge mit Ihren personenbezogenen Daten werden unter Einhaltung der geltenden Vorschriften, insbesondere des französischen Datenschutzgesetzes „Loi Informatique et Libertés" Nr. 78-17 vom 6. Januar 1978 in geänderter Fassung und der Verordnung Nr. 2016/679 des europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr durchgeführt. • Der Flughafen speichert die verarbeiteten Daten so lange, wie es zur Erfüllung der Zwecke der betreffenden Verarbeitung notwendig ist, insbesondere für - die Vornahme und Verwaltung der Buchführung des Unternehmens - die Verwaltung des Betriebs, die Inanspruchnahme von Urlaub und die Entlohnung der Mitarbeiter - die Veranstaltung von Schulungen durch die Mitarbeiter - die Erstattung von beruflich bedingten Aufwendungen der

	Mitarbeiter - die Verwaltung der Nutzung des Telefonsystems des Unternehmens - die Gewährleistung der Sicherheit des Informationssystems - die Gewährleistung der Sicherheit und der Flughafensicherheit zum Schutz von Sachen und Personen. • Die Mitarbeiter sind an eine Sicherheits-und Geheimhaltungsverpflichtung gebunden, die auf die Daten, die sie im Rahmen ihrer Tätigkeit verarbeiten, abgestimmt ist.
Einrichtung einer Datenverarbeitung	• Wenn der Mitarbeiter zur Erfüllung seiner beruflichen Aufgaben eine Verarbeitung persönlicher Daten einzurichten hat (beispielsweise die Arbeitnehmer oder die Kunden betreffend), muss er die Sache vorher seinem Vorgesetzten unterbreiten, damit dieser sich vom Datenschutzbeauftragten bestätigen lässt, das die Verarbeitung den geltenden Gesetzen entspricht.
Wahrnehmung der Rechte der Mitarbeiter	• Gemäß dem französischen Datenschutzgesetz Nr. 78-17 vom 6. Januar 1978 in geänderter Fassung und der Verordnung (EU) 2016/679 zum Schutz personenbezogener Daten, die ab 25. Mai 2018 anzuwenden ist, hat jeder Mitarbeiter des Flughafens die folgenden Rechte an seinen Daten: Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung, Widerspruchsrecht, Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit. Es besteht auch die Möglichkeit, Verfügungen für die Speicherung, die Löschung und die Offenlegung der personenbezogenen Daten eines Mitarbeiters nach seinem Tod zu treffen. • Wenn berechtigte Gründe vorliegen, kann jeder Mitarbeiter der Verarbeitung der auf ihn bezogenen Daten widersprechen. • Um diese Rechte geltend zu machen, richten Sie Ihren Antrag bitte zusammen mit einem Ausweispapier an: Service Juridique, Aéroport de Bâle-Mulhouse, BP 60120, F-68304 Saint-Louis Cedex.

IX. Gesetzliche Formalitäten/Datum des Inkrafttretens/Veröffentlichung/Überarbeitung/Sprachen

Gesetzliche Formalitäten	• Die IT-Richtlinie wurde allen zwingend vorgeschriebenen gesetzlichen Formalitäten unterzogen. Sie wurde insbesondere den Gewerkschaftsvertretern, dem *CSE* und dem *CSP* zur Stellungnahme vorgelegt.
Inkrafttreten	• Die Richtlinie tritt am 1. April 2018 in Kraft und gilt unbefristet.

	• Sie ersetzt die bisherige seit 2008 geltende IT-Richtlinie, die damit unwirksam wird.
Veröffentlichung	• Die IT-Richtlinie wird gegen Empfangsbestätigung an jeden Nutzer am Flughafen ausgegeben und im internen Netzwerk des Flughafens bereitgestellt.
Überarbeitung	• Die Richtlinie kann jederzeit geändert oder überarbeitet werden, insbesondere, um sie an die technische Entwicklung anzupassen oder mit geänderten Gesetzen in Einklang zu bringen.
Sprachen	• Diese Richtlinie wurde in französischer und in deutscher Sprache verfasst. Bei Unstimmigkeiten zwischen diesen beiden Fassungen ist allein die französische Fassung maßgeblich, da die deutsche Fassung eine Höflichkeitsübersetzung ohne Rechtsverbindlichkeit ist.

Erstellt in dreifacher Ausfertigung, Basel, den 22. Februar 2018

Herr Matthias Suhr

Direktor

Herr Frédéric Velter

Stellvertretender Direktor

Frau Elodie Caizergues

HR Direktor