FAQ zur Daten- und Anwendungssicherheit von Factbird

Dieses Dokument dient als Überblick über die Datensicherheit und wie Factbird Daten verarbeitet und speichert. Für weitere Fragen steht Ihnen Factbird jederzeit zur Verfügung.

E-Mail: support@factbird.com

1 Allgemeine Informationen 3
2 Sicherheitsrichtlinien und -verfahren 3
3 Personal 4
4 Sicherheit des Rechenzentrums 4
5 Netzwerk- und Betriebssicherheit 5
6 Zugriffssteuerung 7
7 Incident management 7
8 Backup, Geschäftskontinuität und Notfallwiederherstellung 8
9 Drittanbietersicherheit 8
10 Sicherung 9

1 Allgemeine Informationen

1.1 Name des Unternehmens:

Factbird ApS

1.2 Land des Unternehmens:

Dänemark

1.3 Physische Adresse des Unternehmens:

Nyropsgade 37, 3rd Floor, 1602 Copenhagen V, Denmark

1.4 Welche Art von Cloud nutzt Factbird?

Factbird nutzt eine von AWS (Amazon Web Services) gehostete öffentliche Cloud, die auf den einzelnen Kunden beschränkt oder nicht beschränkt sein kann. In allen Fällen sind die Daten jedoch streng auf den einzelnen Kunden beschränkt. Für große Installationen bieten wir auch eine benutzereigene AWS-Cloud an.

1.5 Auf welcher Art von Cloud-Computing-Modell basiert die Lösung?
A.1 Software-as-a-Service (SaaS).

1.6 Werden die Factbird-Sensordaten über das kundeneigene Netzwerk übertragen?
A.1 Factbird-Daten können entweder über das kundeneigene Netzwerk, über einen separaten WLAN-Hotspot oder über das in der Factbird-Hardware integrierte Mobilfunknetz übertragen werden.

1.7 Stehen externe Auditberichte zur Verfügung?
1.8 Ja. Bitte wenden Sie sich an *support@factbird.com* wenn Sie diese sehen möchten oder daran interessiert sind, selbst ein Audit durchzuführen.

2 Sicherheitsrichtlinien und -verfahren

2.1 Does your organization have documented and approved information Verfügt Ihr Unternehmen über dokumentierte und genehmigte Informationssicherheits- und Datenschutzrichtlinien und -standards, welche die Sicherheitskontrollen für die Informationssysteme und die Verhaltensregeln für Individuen, die auf die Informationssysteme zugreifen, beschreiben?
A.1 Ja, derartige Dokumente liegen vor und Mitarbeiterverträge enthalten klare Regeln hinsichtlich der Vertraulichkeit und damit verbundenen finanziellen Sanktionen für den Einzelnen.

2.2 Verfügt Ihr Unternehmen über ein Risikomanagementprogramm, das Informationssicherheitsrisiken identifiziert, verwaltet und verfolgt?
A.1 Ja, es wird als ein fester Tagesordnungspunkt bei der Vorstandssitzung (mindestens vierteljährliche Sitzungen) geprüft.

2.3 Verfügt Ihr Unternehmen über ein Vulnerabilitätsmanagementprogramm, das Vulnerabilitäten in IT-Systemen identifiziert, verwaltet und verfolgt?
A.1 Ja, Probleme werden in unserem Managementsystem protokolliert und weiterverfolgt.

2.4 Verfügt Ihr Unternehmen über ein Sicherheitsbewertungsprogramm, um implementierte Sicherheitskontrollen zu bewerten und die Wirksamkeit von Sicherheitskontrollen und Schutzmaßnahmen zu evaluieren und ggf. zu verbessern?

A.1 Wir nutzen sowohl die von AWS bereitgestellten Tools als auch ein weiteres Tool, das von einem externen US-Unternehmen bereitgestellt wird, um unsere Sicherheitslage kontinuierlich zu bewerten.

3 Personal

3.1 Werden Mitarbeiter, Auftragnehmer, Drittparteien und vorübergehend Beschäftigte auf die Sicherheitsrisiken im Zusammenhang mit ihren Aktivitäten und die geltenden Sicherheitsstandards aufmerksam gemacht und müssen sie eine Vertraulichkeitsvereinbarung unterzeichnen und sich an die Sicherheits- und Datenschutzrichtlinien des Unternehmens halten?

A.1 Ja. Wir haben keine externen Software-Vertragspartner, eigene Mitarbeiter werden bei der Einarbeitung geschult.

3.2 Gibt es ein formelles Disziplinarverfahren für Mitarbeiter, Auftragnehmer, Drittparteien oder vorübergehend Beschäftigte, die gegen die Unternehmensrichtlinien und -verfahren verstoßen haben?

A.1 Ja. Es sind Strafen in die Mitarbeiterverträge eingebettet.

3.3 Sind Mitarbeiter, Auftragnehmer, Drittparteien und vorübergehend Beschäftigte verantwortlich für den Umgang mit sensiblen Informationen oder managen sie kritische Systeme, Anwendungen oder Netzwerke, die einer Hintergrundprüfung und Sicherheitsüberprüfung unterliegen, bevor sie dafür eingesetzt und mit diesen Verantwortlichkeiten betraut werden.

A.1 Ja. Wir überprüfen ihre Ausbildungsunterlagen. Die Art der Informationen, mit denen wir arbeiten, sind keine Hochrisikodaten.

3.4 Gibt es Verfahren, die den rechtzeitigen Entzug von Zugriffsrechten und die Rückgabe von Vermögenswerten sicherstellen, wenn Mitarbeiter, Auftragnehmer, Drittparteien und vorübergehend Beschäftigte ihren Aufgabenbereich wechseln oder die Organisation verlassen?

A.1 Ja, wir haben ein Formular zur Abmeldung, das von dem ausscheidenden Mitarbeiter unterschrieben wird – das Verfahren wird von unserer Rechtsabteilung unterstützt.

4 Sicherheit des Rechenzentrums

4.1 Befinden sich alle Produktions- und Test Computer-/Serveranlagen im Rechenzentrum/in den Rechenzentren?

A.1 Alle Server sind Cloud-basiert und werden von Amazon Web Service gehostet.

4.2 Gibt es eine Notstromversorgung und unterbrechungsfreie Stromversorgung (UPS – Uninterruptible Power Supply)?

A.1 AWS verfügt über erstklassige Redundanzen zur Sicherstellung der Verfügbarkeit.

4.3 Unterliegt das Rechenzentrum/Unterliegen die Rechenzentren jeglichen Sicherheitsaudits, - bewertungen oder -zertifizierungen durch unabhängige Dritte (z.B. SSAE 16, SOC2, ISO 27001, BS25999)? Wenn ja, bitte führen Sie die relevante/n Zertifizierung und Auditberichte auf

A.1 Ja, besuchen Sie dazu bitte https://aws.amazon.com/compliance/programs/

4.4 Erfüllt das Rechenzentrum/Erfüllen die Rechenzentren die Anforderungen für ein Tier-IVRechenzentrum gemäß der Klassifikation des Uptime Institutes (d.h. ein vollständig fehlertolerantes Rechenzentrum)?

A.1 AWS hat sich dazu entschlossen, nicht mit einem zertifizierten Tiering-Level auf Grundlage der Klassifikation des Uptime Institutes zu arbeiten. Wir möchten an dieser Stelle auf das Statement von Amazon verweisen: „AWS betreibt unsere Rechenzentren in Übereinstimmung den Tier-III+- Richtlinien, jedoch haben wir uns entschlossen, nicht mit einem zertifizierten Tiering-Level auf Grundlage der Klassifikation des Uptime Institutes zu arbeiten, um so mehr Flexibilität bei der Erweiterung und Verbesserung der Leistung zu haben. Der Ansatz von AWS für die Leistung der Infrastruktur erkennt die Tiering-Richtlinien des Uptime Institutes an und wendet sie auf unser globales Rechenzentrum-Infrastrukturdesign an, um das höchste Level an Leistung und Verfügbarkeit für unsere Kunden sicherzustellen. AWS nimmt dann Verbesserungen an den vom Uptime Institute bereitgestellten Richtlinien vor, um eine Skalierung für globale Operationen durchzuführen und ein Betriebsergebnis für Verfügbarkeit und Leistung zu erzielen, die bei Weitem das übertreffen, was durch die Tiering-Richtlinien des Uptime Institutes allein erreicht werden würde. Obwohl wir keine Übereinstimmung mit Tier 4 beanspruchen, können wir sicherstellen, dass unsere Systeme eine fehlertolerante Sequenz von Operationen mit selbstkorrigierenden Schutzmaßnahmen aufweisen.“
https://aws.amazon.com/compliance/uptimeinstitute/

5 Netzwerk- und Betriebssicherheit

5.1 Gibt es einen formalen Betriebsänderungs-Managementprozess, um sicherzustellen, dass alle Hardware- oder Softwareänderungen oder -Updates vor ihrer Implementierung getestet, evaluiert und autorisiert werden?

A.1 Zur Verringerung der Anzahl von Programmfehlern und Problemen in der Produktionsumgebung implementiert unsere Entwicklungsabteilung die folgenden Vorgehensweisen:

- **Pull-Request-Prüfungen**: Alle Veränderungen und Entwicklungen werden durch mindestens einen Senior-Entwickler geprüft.
- **Staging-Umgebung**: Vor dem Einsatz werden alle Veränderungen in einer Staging-Umgebung getestet und verifiziert, welche die Bedingungen in einer Produktionsumgebung simuliert.
- **Blue-Green-Deployment**: Diese Technik erhält zwei identische Umgebungen aufrecht – von denen eine inaktiv ist und die andere aktiv. Neue Merkmale werden zunächst in der inaktiven Umgebung implementiert, in welcher abschließende Verifikationen und Tests stattfinden. Wenn alles bestätigt wird, wird die inaktive Umgebung zur aktiven Umgebung umgeschaltet. Sollten Probleme auftreten, ist ein Zurückschalten möglich.

5.2 Sind Sicherheitsmaßnahmen vorhanden, um das Risiko eines unautorisierten Zugriffs zu begrenzen? Zu derartigen Maßnahmen können Netzwerk-Firewalls, Anwendungs-Firewalls, Eindringungserkennungs- oder -verhinderungssysteme (IDS/IPS) und Netzwerksegmentierung zählen, jedoch nicht darauf beschränkt?

A.1 Ja

- Die Sicherheit von Factbird basiert auf AWS IAM mit dem Prinzip der geringsten Berechtigung.
    - Die AWS-Benutzerkonten der Factbird-Mitarbeiter haben nur die Berechtigungen, die sie für ihre Arbeit benötigen.
    - Auf die externe Factbird-Anwendung kann nur zugegriffen werden, wenn man ein authentifizierter Benutzer ist.
    - Interne Factbird-Services bestehen aus einer Reihe unabhängiger Services, die jeweils eine Teilmenge des gesamten Factbird-Feature-Sets ausführen. Jedem Service werden IAM-Berechtigungen auf Basis der geringsten Rechte zugewiesen, so dass er nur über die minimal erforderlichen Berechtigungen verfügt, um zu funktionieren.
    - AWS IAM-Richtlinien werden über Infrastructure-as-Code erstellt und im Rahmen der Codeüberprüfung überprüft.

- Automatische Audit-Scans von Code-Abhängigkeiten sind vorhanden, um das Risiko von bösartigem Code zu begrenzen.
- Server-Patching und physische Sicherheit werden von AWS übernommen. Für weitere Details siehe bitte Da sich AWS auf das Patchen von Servern und die Sicherheit physischer Server konzentriert, können wir uns auf die Anwendungssicherheit konzentrieren.

5.3 Sind Sicherheitsmaßnahmen vorhanden, um das Risiko von schädlichem Code zu begrenzen, z.B. durch die Verwendung von Antivirus-Software und Malware-Schutz?

A.1 Ja. Siehe Antwort oben.

5.4 Gibt es Vorgehensweisen, um sicherzustellen, dass Sicherheitsupdates (Patches) für Betriebssysteme, Datenbanken, Anwendungen und andere Software zeitnah bewertet und implementiert werden?

A.1 Ja, AWS stellt die Wartung der Infrastrukturdienste zur Verfügung, die wir zum Ausführen von Factbird nutzen.

5.5 Erzeugen IT-Systeme Audit-Protokolle in dem Umfang, der erforderlich ist, um die Überwachung, Analyse, Untersuchung und Meldung von ungesetzlichen, unbefugten oder unangemessenen Aktivitäten zu ermöglichen?

A.1 Ja, wir verfügen über die relevanten Protokollierungs-/Prüfpfade strategischer Ereignisse im Factbird-System, z.B. wer Systemeinstellungen ändert, Überwachung der Systemauslastung, Protokolle auf HTTP usw.

5.6 Werden IT-Systeme und Protokolldateien aktiv auf Anzeichen von rechtswidriger, unautorisierter oder unangemessener Aktivität überwacht?

A.1 Ja, die meisten der Protokolle erzeugen Warn-E-Mails an die Entwickler.

5.7 Wird sämtliche Datenkommunikation (außer öffentlich zugänglicher Webseiten) zwischen Benutzern und IT-Systemen oder zwischen unterschiedlichen IT-Systemen über öffentliche Netzwerke übertragen, die vor unerlaubtem Zugriff oder Eingriff geschützt sind (z.B. durch die Verwendung von SSL/TLS oder anderer für die Industrie akzeptabler Methoden)?

A.1 Ja, wir übertragen von Geräten mit MQTT über TLS. In der Cloud-Datenbankumgebung übernimmt AWS die Kommunikation. Alle Daten von AWS an den Benutzer werden über TLS übertragen. Weitere Einzelheiten dazu, siehe https://aws.amazon.com/security/

5.8 Sind Benutzerdaten in IT-Systemen im Rechenzentrum verschlüsselt?

A.1 Ja, verwaltet von AWS.

5.9 Werden alle Datenträger (einschließlich entfernbarer Medien, Festplatten und Backup-Bänder) vor der Entsorgung oder Freigabe zur Wiederverwendung bereinigt oder zerstört, um zu verhindern, dass Daten von ausrangierten Geräten oder Datenträgern wiederhergestellt werden?

A.1 Die Computer/ Mobiltelefone der Mitarbeiter und die Wechseldatenträger werden in Übereinstimmung mit den Sicherheitsrichtlinien unseres Unternehmens gelöscht.

A.2 Alle Daten werden bei AWS, einer Cloud-Umgebung, gespeichert.

5.10 Welche Sicherheitsmaßnahmen wurden in Ihre APIs eingebaut und wie?

A.1 Wir verwenden OAuth und API-Schlüssel, um Berechtigungen für den API-Zugriff auf Dritte zu verwalten.

A.2 Die MQTT-Sicherheit basiert auf Zertifikaten.

A.3 Drittparteien erhalten API-Zugang auf der Grundlage von API-Schlüsseln.

6 Zugriffssteuerung

6.1 Setzt die Anwendung eine strenge Passwortrichtlinie um:
• Mindestlänge von 8 Zeichen
• Enthält 3 von 4 Komplexitätsgraden (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen)
• Anfangs- oder Rücksetz-Passwort muss unmittelbar nach dem nächsten erfolgreichen Einloggen geändert werden

A.1 a, wir verwenden AWS Cognito, was uns das Konfigurieren individueller Anforderungen für jeden Kunden gestattet.

6.2 Bietet die Anwendung Unterstützung für ADFS?

A.1 Ja.

6.3 Unterstützt das System eine Multi-Faktor-Authentifizierung (z.B. Passwort + Token- oder SMSCode)?

A.1 a. Bei Verwendung unserer AD-Integration kann das Active Directory mit einer Multi-Faktor Authentifizierung konfiguriert werden.

6.4 Werden alle Passwörter, die über ein Netzwerk übertragen werden, durch die Verwendung von SSL/TLS oder anderer für die Industrie akzeptabler Methoden verschlüsselt?

A.1 Ja, alle Passwörter und jeder Benutzerzugriff werden mit AWS Cognito abgewickelt. Weitere Einzelheiten dazu, siehe: https://aws.amazon.com/cognito/

A.2 Der Transport zum und vom AWS-Netzwerk ist verschlüsselt.

6.5 Werden alle Passwörter unter Verwendung eines nicht-reversiblen Verschlüsselungsalgorithmus (z.B. sicherer Passwort-Hash) verschlüsselt im System gespeichert)?

A.1 Ja.

6.6 Kann die Anwendung so eingestellt werden, dass sie einen Benutzer nach einem vordefinierten Zeitraum der Inaktivität automatisch aus der Anwendung abmeldet?

A.1 Ja, dies kann als eine Unternehmensbedingung eingerichtet werden, jedoch kann es nicht für den Benutzer individualisiert werden, es heißt also alle oder keiner.

6.7 Ist der Anmeldemechanismus vor Brute-Force-Angriffen auf Passwörter geschützt (z.B. durch Kontosperrung, Wartezeit zwischen Anmeldungen, CAPTCHA oder ähnliches)?

A.1 Ja.

6.8 Kann die Anwendung so eingestellt werden, dass ein Konto nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche gesperrt wird?

A.1 Ja.

6.9 Müssen Systemadministratoren und anderes Personal mit privilegierten Benutzerrechten, die für den Anbieter arbeiten, eine Zwei-Faktor-Authentifizierung und VPN oder ähnliches verwenden, wenn sie sich für Wartungs- und Support-Zwecke aus der Ferne mit Systemen verbinden.

A.1 Ja.

7 Incident Management

7.1 Gibt es ein formelles Verfahren zur Reaktion auf Informationssicherheitsvorfälle und zur Eskalation, das überprüft, gepflegt und dokumentiert wird?

A.1 Ja, Vorfälle werden in unserem Managementsystem protokolliert und es erfolgen vierteljährliche Prüfungen durch den Vorstand.

7.2 Existiert eine Meldeprozedur, um sicherzustellen, dass der Kunde in Situationen, in welchen die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten beeinträchtigt werden oder worden sein könnte, ohne unnötige Verzögerung benachrichtigt wird?

A.1 Ja, und wir haben eine Methode zur raschen Weiterleitung von Informationen an alle relevanten Nutzer eingerichtet.

8 Backup, Geschäftskontinuität und Notfallwiederherstellung

8.1 Liegen Systeme und Vorgehensweisen vor, um eine Unterbrechung aufgrund von Datenverlust oder Systemausfall zu minimieren (z.B. Backup- und Wiederherstellungssysteme und - prozeduren und/oder Datenduplikation und automatisches Failover)?

A.1 Ja, Factbird führt tägliche automatische Backups aller Produktionsdaten mittels AWS durch. Weitere Einzelheiten dazu finden Sie hier: https://aws.amazon.com/dynamodb/backup-restore/

8.2 Werden Backup-Medien an einem sicheren externen Standort gelagert?

A.1 Ja, AWS verwendet erstklassige Standards für Datensicherheit und Plattformredundanz. Weitere Einzelheiten dazu, siehe Link oben.

8.3 Werden alle Backup-Medien, die möglicherweise Kundendaten enthalten, verschlüsselt?

A.1 Ja, alle gespeicherten Daten sind verschlüsselt; all das wird durch AWS abgewickelt. Weitere Einzelheiten dazu, siehe: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html

8.4 Gibt es für den Fall einer Katastrophe größeren Ausmaßes einen Geschäftskontinuitäts- und Notfallwiederherstellungsplan?

A.1 Ja, aufgrund der Cloud-basierten Natur von AWS und der Blackbird-Anwendung liegen im Fall einer Katastrophe größeren Ausmaßes mehrere Redundanzen vor. Weitere Einzelheiten dazu, siehe https://aws.amazon.com/disaster-recovery/

8.5 Wurden die Geschäftskontinuitäts- und Notfallwiederherstellungspläne innerhalb der letzten 12 Monate evaluiert und getestet?

A.1 Ja, wir haben eine Wiederherstellung basierend auf Rohdaten durchgeführt, und siehe bitte auch die Antwort zu 8.4.

8.6 Verfügen Sie über ein alternatives Rechenzentrum, in dem Sie im Fall einer Krise Kundendaten und Dienste unterbringen könnten? Wenn ja, geben Sie bitte den Standort und den Partner an, der diese Einrichtung betreibt.

A.1 Ja, siehe bitte die Antwort zu 8.4.

9 Drittanbietersicherheit

9.1 Stellen Sie sicher, dass Drittanbieter und Unterauftragnehmer, die Sie zum Bereitstellen von Diensten an die Kunden in Anspruch nehmen, adäquate Sicherheitsmaßnahmen zum Schutz von Informationen, Anwendungen und/oder Diensten einsetzen (z.B. durch Audits, Bewertungen und Vertragsanforderungen)?

A.1 Wir nehmen zwei Dienstanbieter in Anspruch:
AWS – Datendienste werden durch AWS bereitgestellt, sie sind führend im Bereich der Cloud-Computing-Dienste und erfüllen die höchsten Branchenstandards.

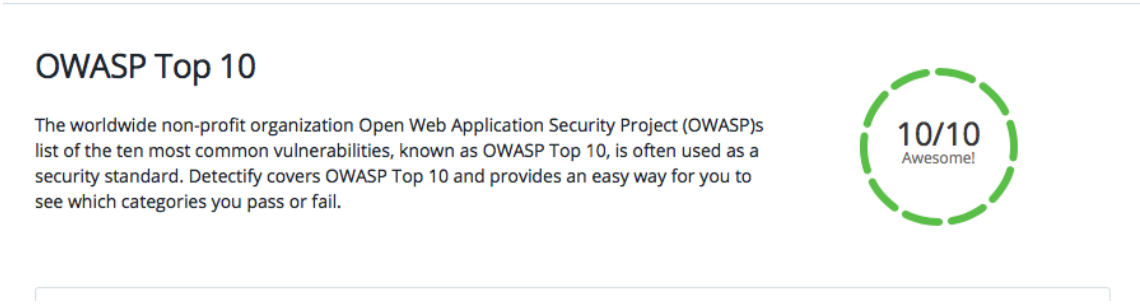
10 Sicherung

10.1 Unterliegt Ihr Unternehmen jeglichen Sicherheitsaudits, Bewertungen oder Zertifizierungen durch unabhängige Dritte (z.B. SSAE 16, SOC2, ISO 27001)?

A.1 Nein.

10.2 Unterliegen Systeme und Anwendungen regelmäßigen Vulnerabilitäts- / Penetrationstests, die durch unabhängige Dritte durchgeführt werden?

A.1 Ja. Ja. Factbird verwendet Detectify zum Durchführen derartiger Tests im Wochenrhythmus. Das System scannt für 500+ bekannte Angriffe und fügt beständig weitere hinzu. Wir werden automatisch über potenzielle Vulnerabilitäten benachrichtigt. Weitere Einzelheiten dazu, siehe: https://detectify.com/ Unsere aktuelle OWASP Top 10 Bewertung ist 10/10 auf unserer Hauptseite cloud.factbird.com laut Detectify:



10.3 Stellt Ihr Unternehmen dem Kunden auf Anfrage ausreichend Informationen zur Verfügung, um es dem Kunden zu ermöglichen, sicherzustellen, dass die angemessenen technischen und organisatorischen Sicherheitsmaßnahmen implementiert wurden (z.B. in Form von Beschreibungen und Dokumentation von Sicherheitsmaßnahmen und/oder Zertifizierungen oder Auditberichten Dritter)?

A.1 Ja.

10.4 Ist es für den Kunden, auf eigene Kosten, möglich, einen Experten mit der Durchführung eines Audits Ihrer Datenverarbeitungseinrichtungen und entsprechender Dokumentation zu beauftragen, um sicherzustellen, dass angemessene technische und organisatorische Sicherheitsmaßnahmen implementiert wurden? (Der Experte wird alle Informationen, die er vom Anbieter erhält oder empfängt, vertraulich behandeln und seine Schlussfolgerungen lediglich an den Kunden weitergeben.)?

A.1 Ja, bitte kontaktieren Sie support@factbird.com

10.5 Ist es möglich, alle Kundendaten regelmäßig in einem lesbaren Format zu exportieren/herunterzuladen, um eine Verfügbarkeit der Daten sicherzustellen, falls das System/der Dienst aus egal welchem Grund ausfällt (Hinterlegung von Daten/Data Escrow)?

A.1 Ja.

10.6 Ist Factbird mit den allgemeinen Datenschutzbestimmungen der EU (GDPR) konform?

A.1 Überblick: Factbird speichert keine sensiblen personenbezogenen Daten. Factbird speichert jedoch personenbezogene Daten in Form von E-Mails, Namen, Abonnements und Zugriffen sowie Daten, die von Nutzern in einfachen Textfeldern hinterlassen werden. Diese Daten werden mit äußerster Sorgfalt behandelt und niemals an Dritte weitergegeben.

A.2 Benachrichtigung bei Verstößen: Im unwahrscheinlichen Fall einer Datenschutzverletzung werden die Kunden und die zuständigen Behörden benachrichtigt.

A.3 Recht auf Auskunft: Auf Antrag kann eine betroffene Person neben einer Kopie der Daten auch vollständigen Einblick in die Verwendung ihrer Daten erhalten.

A.4 Recht auf Vergessenwerden: Auf Antrag kann eine betroffene Person ihre personenbezogenen Daten aus dem Factbird-System löschen lassen.

A.5 Datenübertragbarkeit: Auf Antrag kann eine betroffene Person eine elektronische Kopie ihrer Daten in einem gängigen elektronischen Format erhalten.

A.6 Datenschutz durch Design: Factbird beschränkt den Zugriff auf personenbezogene Daten auf diejenigen, die den Zugriff für geschäftskritische Verarbeitungen benötigen. Factbird verarbeitet oder speichert keine Daten, die nicht für die geschäftlichen Bedürfnisse des Kunden relevant sind.

A.7 Datenschutzbeauftragte: Factbird hat Nicole Sowe, Emendo Consulting, Dänemark, zur Datenschutzbeauftragten ernannt.