# Dataskyddsbilaga ("Bilaga") till Orderformulär

1 Denna dataskyddsbeskrivning gäller som länkad till orderformuläret (inklusive affärsresevillkoren och/eller villkoren för mötes- och evenemangstjänster, beroende på vad som är tillämpligt) (gemensamt "avtalet") mellan Reed & Mackay Sverige AB ("R&M") (registrerat i Sverige under nr 556164-4260) med säte på Box 1114, 405 23 Göteborg och dig som kund. Definierade termer som används på andra ställen i Avtalet ska ha samma betydelse i detta Tillägg. När R&M behandlar Data som personuppgiftsbiträde för Kundens räkning ska R&M

1.1 endast använda uppgifterna för att:

(a) fullgöra sina skyldigheter enligt detta avtal och behandla sådana uppgifter i enlighet med kundens skriftliga instruktioner; och/eller

(b) följa Dataskyddslagstiftningen eller lagarna i någon annan medlemsstat i Europeiska Unionen (förutsatt att R&M, före den relevanta behandlingen, har informerat Kunden om ett sådant krav (såvida inte den Relevanta Lagen förbjuder ett sådant meddelande));

1.2 med förbehåll för punkterna 2, 4 och 5 (inklusive) i denna Bilaga, implementera och upprätthålla lämpliga tekniska och organisatoriska åtgärder för att skydda Data som behandlas i samband med detta Avtal från oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt röjande eller obehörig åtkomst och vidta alla åtgärder som krävs enligt artikel 32 i GDPR ("säkerhet vid behandling") (eller motsvarande krav enligt Dataskyddslagstiftningen i Sverige i den mån GDPR upphör att gälla direkt i Sverige);

1.3 vidta alla rimliga åtgärder för att säkerställa tillförlitligheten hos alla R&M-anställda som har tillgång till Data som behandlas i samband med detta avtal och säkerställa att alla sådana R&M-anställda är bundna av verkställbara sekretessförpliktelser;

1.4 med beaktande av behandlingens art, bistå Kunden med lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, för fullgörandet av Kundens skyldighet att besvara förfrågningar från registrerade som utövar sina rättigheter enligt kapitel III i GDPR;

1.5 bistå Kunden med att säkerställa att Kunden fullgör sina skyldigheter enligt artiklarna 32-36 i GDPR ("säkerhet vid behandling", "anmälan av personuppgiftsincident ...", "konsekvensbedömning avseende dataskydd" och "förhandssamråd"), med beaktande av behandlingens art och den information som R&M har tillgång till;

1.6 meddela kunden utan onödigt dröjsmål och under alla omständigheter inom 48 timmar efter att ha fått kännedom om ett säkerhetsbrott som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt avslöjande av eller tillgång till data som behandlas av R&M i samband med detta avtal;

1.7 inom rimlig tid efter meddelande från Kunden, tillhandahålla Kunden all information som är nödvändig för att visa att de skyldigheter som anges i detta Tilläggsavtal uppfylls och tillåta och bidra till revisioner, inklusive inspektioner, som utförs av Kunden eller annan revisor som utsetts av Kunden, förutsatt att sådana revisioner och/eller inspektioner endast sker vid ett (1) tillfälle under en tolvmånadersperiod, att sådana inspektioner och/eller revisioner är strikt begränsade till R& M:s arrangemang för att uppfylla detta Tilläggsavtal och att sådana inspektioner och/eller revisioner utförs under normal arbetstid och att Kunden (eller relevant tredje part som utför en sådan revision) skriftligen meddelar R& M om en sådan revision och/eller inspektion. R&M's arrangemang för efterlevnad av detta Tillägg, att sådana inspektioner och/eller revisioner utförs under normala affärstider och att Kunden (eller den relevanta tredje part som utför en sådan revision) skriftligen ger R&M rimlig förvarning om en sådan revision och/eller inspektion och att omfattningen av en sådan revision och/eller inspektion avtalas med R&M innan den påbörjas;

1.8 ha rätt att överföra Data utanför det Europeiska ekonomiska samarbetsområdet förutsatt att lämpliga skyddsåtgärder finns på plats enligt dataskyddslagstiftningen, inklusive utan begränsning där så är lämpligt: (a) för överföringar av Data från det Europeiska ekonomiska samarbetsområdet, EU:s standardavtalsklausuler finns på plats; eller (b) någon annan giltig överföringsmekanism finns på plats enligt dataskyddslagstiftningen. För att undvika tvivel och med förbehåll för punkt 4 nedan, bekräftar och godkänner Kunden att R&M inte är skyldigt att ingå några standardavtalsklausuler (inklusive utan begränsning EU:s standardavtalsklausuler) eller andra avtal med Tjänsteleverantörer;

1.9 omedelbart meddela Kunden om R&M anser att någon instruktion eller anvisning från Kunden strider mot dataskyddslagstiftningen eller annan tillämplig dataskyddslagstiftning i EU eller medlemsstat; och

1.10 efter Kundens val, radera eller återlämna all Data till Kunden när Tjänsterna upphör att tillhandahållas Kunden, och radera alla då befintliga kopior (såvida inte R&M måste behålla dessa enligt tillämplig lag).

2 Kunden bekräftar och samtycker till, och ska se till att resenärerna och användarna bekräftar och samtycker till, att det är nödvändigt för R&M att tillhandahålla Data till tjänsteleverantörer (oavsett om de befinner sig inom EES eller inte) för att kunna tillhandahålla Tjänsterna.

3 Kunden bekräftar och samtycker till att R&M ska ha rätt att använda Underbiträden i samband med behandlingen av Data för Kundens räkning för tillhandahållandet av Tjänsterna enligt detta Avtal. En lista över underbiträden som används av R&M finns tillgänglig här.

R&M ska informera kunden om eventuella ändringar i listan över underbiträden, inklusive tillägg av nya underbiträden. Om Kunden motsätter sig en ändring av listan över Underbiträden ska Kunden skriftligen meddela R&M inom 15 dagar från det att den uppdaterade listan över Underbiträden publicerats. Om Kunden lämnar ett sådant meddelande till R&M kommer R&M, om möjligt, att fullgöra sina skyldigheter enligt detta Avtal utan att Data i samband med detta Avtal behandlas av de nya Underbiträdena. Om det emellertid inte är rimligt möjligt för R&M att fullgöra sina skyldigheter enligt detta Avtal utan att de nya Underbiträdena behandlar Data i samband med detta Avtal, ska R&M meddela Kunden om detta och Kunden ska ha rätt att säga upp detta Avtal med trettio (30) dagars skriftligt varsel till R&M. Om Kunden inte invänder mot någon ändring eller tillägg till listan över Underbiträden inom 15 dagar från det att den uppdaterade listan publicerats av R&M, ska Kunden anses ha godkänt alla ändringar och/eller tillägg till listan över Underbiträden. R&M förblir ansvarigt och skadeståndsskyldigt för alla handlingar eller försummelser av dess Underbiträden. R&M ska säkerställa att det finns ett skriftligt avtal med underbiträdena som innehåller villkor för skydd av Data som inte är mindre skyddande än de villkor som anges i detta Tillägg.

4 Utan att det påverkar tillämpningen av punkt 2 ovan, och utan hinder av någon annan bestämmelse i detta avtal, ska kunden:

(a) samtycker härmed till att R&M överför Data till en Tjänsteleverantör (oavsett om denna befinner sig inom EES eller inte) i syfte att tillhandahålla Tjänsterna i enlighet med detta Avtal; och

(b) ska tillse att Resenärerna och Användarna, där så är nödvändigt, var och en har gett sitt samtycke till att R&M överför Resenärernas och Användarnas Data till Tjänsteleverantörer i syfte att tillhandahålla Tjänsterna i enlighet med detta Avtal.

5 Mot bakgrund av punkt 2 ovan ska R&M göra vad som rimligen kan krävas för att hjälpa Kunden att reagera på en Tjänsteleverantörs underlåtenhet (vare sig handling eller underlåtenhet) att behandla Data i enlighet med lämpliga och branschstandardiserade metoder. R&M ska i övrigt inte ha något ansvar gentemot Kunden, någon medlem av Kundens Grupp eller någon Resenär eller Användare (vare sig i kontrakt, skadestånd (inklusive försumlighet eller brott mot lagstadgad skyldighet), felaktig framställning eller på annat sätt) som uppstår på grund av eller i samband med att någon Tjänsteleverantör behandlar, använder, missbrukar, förlorar, skadar eller förvanskar Data, eller på annat sätt gör intrång i en persons rättigheter i förhållande till Data.

6 Utan att det påverkar tillämpningen av punkterna 2, 4 och 5 ovan (inklusive) i detta Tillägg, ska Kunden säkerställa att alla nödvändiga rättsliga grunder finns på plats, inklusive, i förekommande fall, inhämtande av samtycke, och ska förse Resenärer och Användare med all nödvändig information för att möjliggöra att Data lagligen kan tillhandahållas R&M i enlighet med Dataskyddslagstiftningen.

7 Kunden är medveten om och godkänner att Bilaga 1 till denna Bilaga innehåller vissa detaljer rörande R&M:s behandling av data i enlighet med detta Avtal.

8 Kunden bekräftar och samtycker till att bära kostnaden för, och ersätta R&M för, rimliga kostnader och utgifter som R&M ådrar sig för att tillhandahålla assistans enligt punkterna 1.4 och 1.5 ovan.

9 Om inte annat följer av tillämplig lag ska R&M: (i) utan onödigt dröjsmål informera Kunden om varje begäran, order eller liknande krav från en domstol, behörig myndighet, brottsbekämpande eller annat statligt organ ("begäran om brottsbekämpning") avseende behandlingen av Data enligt detta Avtal och ge Kunden möjlighet att invända mot varje sådan begäran om brottsbekämpning; och (ii) vidta rimliga åtgärder för att förhindra att Data som behandlas av R&M enligt detta Avtal lämnas ut som svar på en begäran om brottsbekämpning utan Kundens uttryckliga skriftliga medgivande i förväg.

**Bilaga 1**

**Aktiviteter för databehandling**

| | |
|---|---|
| Kategorier av data | Uppgifter om resenären och/eller bokaren - titel, förnamn, mellannamn, efternamn, känt namn (om annat), kön, födelsedatum, födelseort och födelseland, bosättningsland, nationalitet, civilstånd; resenärens plats - destinationer och platser på resan.<br><br>Företagsinformation - företagsnamn, avdelning, kostnadsställe, kontonummer, jobbtitel, anställningsnummer<br><br>Huvudsakliga kontaktuppgifter - adresser (hem, kontor etc.), telefonnummer, faxnummer, mobiltelefonnummer, e-postadress<br><br>Information om resebokare/PA - namn, telefonnummer, e-postadress<br><br>Betalningsmetoder - korttyp, kortnummer, utgångsdatum, användningspreferenser, debitering/kredit, personligt/företag<br><br>Dokument -<br>Pass - passland, utfärdandeland, passnummer, förnamn, mellannamn, efternamn, utfärdandedatum, sista giltighetsdag, biometriska uppgifter (J/N)<br>Visering (inklusive ESTA, Redress, Schengen, arbetstillstånd, Global Entry) - viseringsland, utfärdandeland, typ av visering, dokumentnummer, utfärdandedatum och sista giltighetsdag<br>TSA - TSA-nummer, startdatum, utgångsdatum<br>Körkort - land, körkortsnummer, förnamn, mellannamn, efternamn, startdatum, utgångsdatum, provisoriskt (J/N), internationellt (J/N)<br>ID-kort - land, ID-kortsnummer, förnamn, mellannamn, efternamn, startdatum, utgångsdatum<br>Vaccin-, Covid- och hälsoinformation som krävs för bokningar<br><br>Resepreferenser -<br>Flyg - typ av säte, hemflygplats, önskemål om incheckning online, typ av måltid<br>Bil - kategori, modell, växellåda, bränsle/luftkonditionering, satellitnavigering (J/N),<br>Tåg - platstilldelning, typ av måltid<br>Eurostar - bussnummer, platsnummer, typ av plats, platstilldelning, typ av måltid<br>Hotell - rökning/icke-rökning, önskad rumstyp<br>Eventuella tillgänglighetskrav för resan<br><br>Medlemskap - lojalitetskort - typ av tjänst, leverantör, medlemsnummer, utgångsdatum, status, nivå<br><br>Personliga hobbyer/intressen |
| Kategorier av registrerade | Anställda och gäster hos kunden och andra för vilka kunden kräver resor |
| Bearbetning av uppgifter | Tillhandahållande av resor och reserelaterade tjänster |
| Syfte | Tillhandahållande av resor och reserelaterade tjänster |
| Varaktighet | Ekonomi - kontraktets löptid + 7 år<br>Profiler - under avtalstiden, granskas årligen och raderas på begäran av kunden |

**Bilaga 2**

**EU:s standardavtalsklausuler (Modul 2 - Personuppgiftsansvarig till personuppgiftsbiträde)**

Startdatum: Enligt vad som anges i Avtalet

| Exportör *(som skickar den Begränsade överföringen):* | Importör *(som tar emot den Begränsade överföringen):* |
|---|---|
| Kunden, enligt vad som anges i Avtalet | Reed & Mackay Sverige AB, i enlighet med vad som anges i Avtalet |
| Viktig kontaktperson:<br>Fullständigt namn:<br>Arbetstitel:<br>Kontaktuppgifter: | Viktig kontaktperson:<br>Fullständigt namn:<br>Arbetstitel:<br>Kontaktuppgifter: |
| Underskrift: | Underskrift: |

**1. Modellklausuler**

För detta avtals syften skall modellklausulerna införlivas enligt följande:

| Modul i drift: | Klausul 7 (Dockningsklausul) | Klausul 9a (Förhandsgodkännande eller generellt godkännande) | Paragraf 9a (Tidsperiod) | Paragraf 11 (Option) | Paragraf 17 (Option) | Paragraf 18 (Option) |
|---|---|---|---|---|---|---|
| 2 | Inkorporerad | Allmän auktorisation | 15 dagar | Inkorporerad | Lagstiftningen i en EU-medlemsstat där uppgiftsutföraren är etablerad | Republiken Irland |

| Tillämpliga klausuler | Alla klausuler som utarbetats inom Modul två: Överföring av personuppgiftsansvarig till personuppgiftsbiträde, av de standardavtalsklausuler som godkänts av Europeiska kommissionens beslut 2021/914 av den 4 juni 2021; är tillämpliga enligt utkast. |
|---|---|

**2. Bilaga Information**

Enligt vad som anges i tillägget till detta schema nedan.

**Bilaga 2 - Tillägg 1**

**Beskrivning av överföringen**

**Kategorier av registrerade vars personuppgifter överförs**

Enligt vad som anges i bilaga 1 under "Kategorier av registrerade".

**Kategorier av personuppgifter som överförs**

Enligt vad som anges i bilaga 1 under "Kategorier av uppgifter".

**Känsliga uppgifter överförs (om tillämpligt) och restriktioner eller skyddsåtgärder tillämpas som fullt ut tar hänsyn till uppgifternas art och de risker som är förknippade med dem, t.ex. strikt begränsning av syftet, åtkomstbegränsningar (inklusive åtkomst endast för personal som har genomgått specialutbildning), registrering av åtkomst till uppgifterna, begränsningar för vidareöverföringar eller ytterligare säkerhetsåtgärder.**

R&M behandlar inte rutinmässigt uppgifter i särskilda kategorier. När det gäller den resetjänst som tillhandahålls kan känsliga uppgifter härledas, t.ex. när assistans krävs (vilket kan innebära hälsotillstånd), information om vaccin och/eller tester (som krävs för bokningar, vilket kan innebära hälsostatus) och måltidspreferenser (från vilka religion kan härledas). R&M tillämpar samma höga nivå av säkerhetsåtgärder för alla personuppgifter.

**Hur ofta överföringen sker (t.ex. om uppgifterna överförs vid ett enstaka tillfälle eller kontinuerligt).**

Överföringen sker fortlöpande i syfte att tillhandahålla resor och reserelaterade tjänster.

**Typ av behandling**

Enligt vad som anges i bilaga 1 under "Behandlingar".

**Ändamål med överföringen och den fortsatta behandlingen av uppgifterna**

Enligt vad som anges i bilaga 1 under "Ändamål"

**Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period**

Enligt vad som anges i bilaga 1 under "Varaktighet".

**För överföringar till (under-)personuppgiftsbiträden, ange även ämne, typ och varaktighet för behandlingen**

https://clientportal.reedmackay.com/account/privacyandcookies

**Identifiera den behöriga tillsynsmyndigheten/tillsynsmyndigheterna i enlighet med klausul 13**

Irländska dataskyddsmyndigheten

**Bilaga 2 - Tillägg 2**

Tekniska och organisatoriska åtgärder, inklusive tekniska och organisatoriska åtgärder för att säkerställa datasäkerheten

***Version 2.5 - juli 2024 (som kan komma att uppdateras av R&M från tid till annan)***

## DEFINITIONER

Med "personal" avses Reed & Mackays anställda, uppdragstagare eller konsulter som är involverade i den tjänst Reed & Mackay tillhandahåller sina kunder.

"Data" avser klientdata som tillhandahålls Reed & Mackay av klienten (personuppgiftsansvarig) i enlighet med eventuella personuppgiftsbiträdesavtal och/eller avtal mellan klienten och Reed & Mackay.

## INLEDNING

Ledningen för Reed & Mackay är medveten om betydelsen av informationssäkerhet och att upprätthålla högsta standard avseende sekretess, integritet och tillgänglighet för intern information, kund- och leverantörsinformation är grundläggande för vår vision "Att vara det mest uppskattade, rekommenderade och entreprenörsdrivna rese-, rådgivnings- och eventföretaget i världen".

Som beskrivs i detta dokument upprätthåller Reed & Mackay en uppsättning tekniska och organisatoriska säkerhetsåtgärder i linje med branschens bästa praxis och standarder och certifieringar som vi upprätthåller för att minska riskerna för data, informationstillgångar, service, prestanda, kundförtroende eller andra delar av verksamheten som kan uppstå till följd av en brist i informationssäkerheten.

## 1. CERTIFIERINGAR

1.1. Reed & Mackay upprätthåller ISO/IEC 27001, den internationella standarden för hantering av informationssäkerhet, ISO 22301 - Business Continuity Management, ISO 9001 - Quality Management, och ISO 14001 - Environmental Management certifieringar. Reed & Mackay är också certifierat enligt PCI-DSS - The Payment Card Industry - Data Security Standard, vilket också är en förutsättning för IATA-licensiering och därför tas på största allvar av Reed & Mackay.

1.2. Certifieringarna upprätthålls genom ett externt och ett internt revisionsprogram, som omfattar periodiska interna och årliga externa revisioner samt kontinuerliga förbättringsaktiviteter.

## 2. LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET

2.1. Reed & Mackays informationssäkerhetspolicyer anger en tydlig riktning för informationssäkerheten och visar stöd för och engagemang i hanteringen av informationssäkerheten inom hela företaget.

2.2. Informationssäkerheten hanteras genom en strikt uppsättning kontroller, inklusive policyer, processer, rutiner, program- och maskinvarufunktioner som utgör Reed & Mackays ledningssystem för informationssäkerhet (ISMS). Dessa kontroller övervakas, granskas och förbättras vid behov för att säkerställa att specifika säkerhets- och affärsmål uppfylls.

2.3. All personal får ett omfattande och obligatoriskt introduktions- och utbildningsprogram när de börjar på företaget och en årlig uppdatering av efterlevnaden, inklusive informationssäkerhet och dataskydd.

2.4. Det yttersta ansvaret för informationssäkerheten ligger hos Chief Information Officer, men detta ansvar fullgörs genom den utsedda rollen som Director of Security & Trust, som har huvudansvaret för informationssäkerhet, informationssäkerhetsrisker, cybersäkerhet och hantering av säkerhetsincidenter inom Reed & Mackay och fungerar som den centrala kontaktpunkten för informationssäkerhet för både personal och externa organisationer.

2.5. Avdelningscheferna ansvarar för att informationssäkerhetspolicyn tillämpas inom deras affärsområden och för att personalen följer den. All personal har ett ansvar för informationssäkerheten; att säkerställa att de följer relevanta företagspolicyer, processer och rutiner; att de har en allmän medvetenhet om vikten av informationssäkerhet och de potentiella riskerna; att de rapporterar alla incidenter, händelser eller potentiella svagheter.

## 3. SÄKERHET FÖR MÄNSKLIGA RESURSER

3.1. Reed & Mackay har ett nära samarbete med våra kontakter på rekryteringsbyråer för att säkerställa att krav på screening före anställning genomförs för vår räkning.

3.2. Reed & Mackay anlitar ett tredjepartsföretag för att genomföra bakgrundskontroller i enlighet med den brittiska regeringens Baseline Personnel Security Standard (BPSS) av all personal oavsett roll, med förbehåll för begränsningar i enlighet med lokal lagstiftning.

3.3. Sekretessklausuler finns i anställningsavtalen som ger ett adekvat skydd för konfidentialiteten för uppgifterna.

3.4. En disciplinär process finns på plats för att hantera bristande efterlevnad av säkerhetspolicyer och säkerhetskrav.

3.5. Vid anställningens upphörande återkallas personalens tillträde den sista arbetsdagen och all utrustning och immateriella rättigheter återlämnas av den som slutar.

## 4. KAPITALFÖRVALTNING OCH DATASÄKERHET

4.1. Tillgångar som är förknippade med information och anläggningar för informationsbehandling identifieras och en inventering av tillgångarna upprätthålls.

4.2. Information och data klassificeras och hanteras i enlighet med en policy för informationsklassificering, tillgångs- och datahantering som godkänts av ledningen.

4.3. Endast betrodda enheter har tillgång till Reed & Mackays företagsnätverksresurser. Dessa inkluderar Reed & Mackay-domänanslutna datorer och mobila enheter som har registrerats med Reed & Mackays Mobile Device Management Solution och som följer säkerhetspolicyerna.

4.4. Kraven på säkerhetskontroller för personliga och av Reed & Mackay utfärdade mobila enheter definieras i policyn för mobila och personliga enheter. Kontrollerna omfattar, men är inte begränsade till, kryptering, fjärradering och avaktiverade USB-portar.

4.5. Alla slutpunkter är krypterade. USB-portar och användning av flyttbara media är begränsad.

4.6. Tekniska DLP-åtgärder samt en Clear Desk & Clear Screen-policy finns på plats för att minska risken för dataläckage och oavsiktligt utlämnande av data.

4.7. En policy för datalagring och ett schema för datalagring finns på plats för att definiera kraven på datalagring i enlighet med GDPR och dataskyddslagen, samt krav på säker datahantering av känsliga data på fysiska eller elektroniska medier enligt erkända säkerhetsstandarder/best practice för IT-branschen (t.ex. godkända standarder från CESG eller försvarsdepartementet).

4.8. Media som innehåller information förstörs på ett säkert sätt i enlighet med WEEE:s (Waste Electrical and Electronic Equipment) och CESG:s (Communications Electronics Security Group) godkända standarder för datadestruktion. Avdelningen för tekniska tjänster upprätthåller register.

4.9. Dokumentationen förstörs på ett säkert sätt antingen med hjälp av dokumentförstörare eller genom att använda godkända tredje parter som tillhandahåller tjänster enligt BS EN 15713-standarden för säkerhetsfragmentering och minst DIN P-3-säkerhetsnivå, lämplig för konfidentiella dokument.

## 5. TILLGÅNGSKONTROLL

5.1. En modell för rollbaserad åtkomstkontroll finns på plats med roller som tilldelas individer baserat på arbetsuppgifter och behov av att veta.

5.2. Principerna om åtskillnad av arbetsuppgifter och lägsta privilegium följs, och privilegierad åtkomst beviljas efter dokumenterat godkännande av den högsta ledningen.

5.3. Privilegierade IT-administrativa rättigheter tillhandahålls via ett separat användar-ID (förhöjt konto) till användarens normala användar-ID.

5.4. Vi övervakar alla händelser i samband med inloggning på servrar + arbetsstationer med administrativa konton samt ändringar/modifieringar av behörighetsgrupper.

5.5. Granskningar av åtkomsträttigheter genomförs regelbundet och frekvensen beror på hur kritisk informationstillgången är och varierar mellan kvartalsvis och årligen.

5.6. Reed & Mackays lösenordspolicy definieras enligt följande: Lösenord måste innehålla minst 12 tecken, minst en stor bokstav, en liten bokstav och en siffra eller ett specialtecken. Lösenord måste undvika internationella tecken (icke-ASCII), får inte innehålla ordboksord eller information om användaren (t.ex. användar-ID, namn på familjemedlemmar, födelsedatum etc.), ska ändras minst en gång var 90:e dag och får inte vara samma som de 24 tidigare använda lösenorden.

5.7. Användarkonton låses efter 5 ogiltiga inloggningsförsök och förblir låsta tills en administratör eller användaren låser upp dem (det senare sker via självbetjäning och multifaktorautentisering).

5.8. Multifaktorautentisering tillämpas på alla Reed & Mackays användar- och administrativa konton.

## 6. KRYPTERING

6.1. Enligt definitionen i Reed & Mackays krypterings policy används krypterings-kontroller för att skydda känsliga data både under transport och i vila.

6.2. Kryptering på mobila enheter verkställs via policyer för Microsoft Intune Endpoint Manager.

6.3. Kryptering av PII-databasen sker via Thales CipherTrust (AES 256-bitars kryptering, datatokenisering och krypteringstjänster).

6.4. Databaskryptering sker med hjälp av Transparent Data Encryption (TDE) AES-256-kryptering.

6.5. All trafik från/till våra applikationer som vänder sig till allmänheten (webbplatser + mobilapp) använder HTTPS-certifikat som utfärdats av GlobalSign Certificate Authority och krypteras med TLS 1.2 eller högre.

6.6. Alla säkerhetskopior är krypterade.

## 7. SÄKERHET I VERKSAMHETEN

7.1. Förändringar i produktionsmiljöer kontrolleras i enlighet med Reed & Mackays policy för hantering av IT-förändringar.

7.2. Kontrollerna för att upptäcka, förebygga och återställa skadlig programvara finns på plats via nästa generations lösning mot skadlig programvara.

7.3. En omfattande process för patchhantering finns på plats. Patchar och säkerhetsuppdateringar distribueras varje månad, eller oftare om en betydande säkerhetsrisk har identifierats. Patchhanteringen är föremål för ändringskontroll och policyn för hantering av IT-ändringar.

7.4. Ett program för hantering av tekniska sårbarheter finns på plats, inklusive ett löpande program för att åtgärda sårbarheter. Sårbarheter identifieras via interna och externa infrastrukturskanningar, kvartalsvisa PCI-DSS ASV-skanningar och penetrationstester.

7.5. Ett omfattande årligt program för penetrationstest finns på plats och utförs av CREST-ackrediterade oberoende penetrationstestare.

## 8. LOGGNING, ÖVERVAKNING OCH HANTERING AV SÄKERHETSINCIDENTER

8.1. Händelseloggar som registrerar användaraktiviteter, undantag, fel och informationssäkerhetshändelser genereras, bevaras, skyddas från manipulering och granskas regelbundet.

8.2. En 24/7 Security Operations Centre (SOC)-tjänst finns på plats via en betrodd tredjepartsleverantör av Managed Security Services, som omfattar övervakning, loggsamling och analys, SIEM (Security Information & Event Management), svar på och begränsning av säkerhetsincidenter samt kriminalteknisk analys för att förstå orsaken till säkerhetsincidenter och metoder för att minska eller ta bort potentiella områden för angrepp.

8.3. Observerade eller misstänkta säkerhetsincidenter rapporteras centralt, loggas automatiskt och följs upp av Security Incident Response Team i enlighet med Information Security Incident Response Plan och Data Breach Management Process, om tillämpligt.

## 9. CLOUD SÄKERHET

9.1. Reed & Mackays plattform för resehantering och serverinfrastruktur finns i Microsoft Azures datacenter i södra Storbritannien.

9.2. MS Azure är konfigurerat för att kryptera information i vila oavsett lagringsmedium, oavsett om det är en hanterad disk som är kopplad till en virtuell maskin, ett lagringskonto som innehåller telemetridata eller applikationskällkod eller en plattformsdatabastjänst som Microsoft SQL.

9.3. En molnsäkerhetspolicy som godkänts av ledningen finns på plats för att definiera säkerhetskraven för molnet.

9.4. En Cloud Security Posture Management-lösning finns på plats för att övervaka och hantera styrning av Reed & Mackays Microsoft Azure-baserade tillgångar och tjänster, inklusive visualisering och bedömning av säkerhetsläget, upptäckt av felkonfigurationer och tillämpning av bästa praxis för säkerhet och ramverk för efterlevnad.

9.5. Microsoft Network Security Groups och Next Generation Checkpoint virtual firewall appliances skyddar vår miljö på perimetern med Intrusion Prevention aktiverat.

## 10. FYSISK SÄKERHET

10.1. I enlighet med vår policy för fysisk och miljömässig säkerhet finns det lämpliga fysiska och miljömässiga säkerhetsåtgärder på plats för att förhindra obehörig fysisk åtkomst, skada och störning av data, lokaler och behandlingsanläggningar. Följande kontroller finns på plats:

10.1.1. Huvudkontor: Bemannad reception i byggnaden 24x7, Reed & Mackays kontorsreception är öppen under kontorstid. CCTV vid alla byggnadens tillträdespunkter som täcker de flesta gemensamma utrymmena och områdena för in- och utpassering från byggnaden. Tillträde till IT-kommunikationsrummet sker med hjälp av ett system med svepkort och knappsats. Tillträdet är begränsat till behöriga personer med ett affärsbehov.

10.1.2. Regionala kontor: Regionkontoren har samma kontroller som huvudkontoret, med vissa undantag. Våra mindre kontor har inte bemannad reception dygnet runt eller passerkortssystem, men kompenserande kontroller är i linje med vår policy för fysisk och miljömässig säkerhet för att säkerställa att den fysiska säkerheten på dessa kontor är tillräcklig.

10.2. Besökare beviljas endast tillträde för specifika och auktoriserade ändamål och övervakas/ledsagas alltid när de befinner sig på Reed & Mackays kontor. Besöksloggar förs för all fysisk åtkomst till Reed & Mackays kontor, serverrum och datacenter som hyser Reed & Mackays IT-utrustning och informationstillgångar.

## 11. KOMMUNIKATION & NÄTVERKSSÄKERHET

11.1. Nätverken hanteras med hjälp av lämpliga säkerhetskontroller som nätverkssegmentering, hantering av nätverksåtkomst, brandväggar, konfigurationsstandarder samt loggning och övervakning.

11.2. Förfaranden och kontroller för informationsöverföring finns på plats för att skydda överföringen av uppgifter med hjälp av alla typer av kommunikationsmedel.

11.3. Vårt rekommenderade dataöverföringsprotokoll för regelbundna datautbyten (t.ex. datafiler, HR-flöden) är att upprätta en SFTP-anslutning mellan organisationerna - vilken part som skickar/tar emot data är öppet för överenskommelse mellan parterna.

## 12. UTVECKLING AV PROGRAMVARA

12.1. Den interna programvaruutvecklingen följer Agile/Sprint-livscykelmetodiken och följer OWASP:s bästa praxis.

12.2. En SDLC-policy (Software Development Lifecycle) har införts som omfattar kravanalys och specifikationer, inbyggd säkerhet, säkra tekniska principer, säker utvecklingsmiljö, applikationssupport, kvalitetssäkring, testning, implementering, utbildning och granskning efter implementering.

12.3. Integration av Single-Sign-On är tillgänglig i våra kundinriktade applikationer. SAML 2.0-baserade lösningar som Azure AD, Ping Identity, Duo och Okta stöds, andra tredjepartsalternativ kan också stödjas, men kan kräva utveckling och testning.

12.4. Utvecklings-, test- och produktionssystem är åtskilda. Anonymiserade data används för teständamål i miljöer som inte är produktionsmiljöer.

12.5. Kunddata separeras med hjälp av unika identifierare som tilldelas vid tidpunkten för kontoimplementeringen. Segregering säkerställs genom att använda unika identifierare, t.ex. företags-ID, resenärs-ID och konto-ID.

## 13. RELATIONER MED LEVERANTÖRER

13.1. Nya direktleverantörer (inklusive underbiträden) genomgår en due diligence som omfattar informationssäkerhet, dataskydd, kontinuitet i verksamheten, bolagsstyrning och kvalitet, hälsa och säkerhet, miljö, lika möjligheter, mångfald, mutor och korruption, modernt slaveri och barnarbete, etiska affärsmetoder/företagets sociala ansvar samt en kreditupplysning, en

granskning av policyer, certifieringar, oberoende revisionsrapporter, oberoende penetrationstester (inklusive uppföljning av åtgärder) etc. i tillämpliga fall.

13.2. Leverantörerna omfattas av sekretess- och revisionsklausuler i sina avtal.

13.3. Leverantörer måste följa Reed & Mackays principer för leverantörsverksamhet och leverantörer av produkter/tjänster som interagerar med R&M:s informationssystem eller behandlar personuppgifter måste enligt avtal godkänna våra krav på informationssäkerhet för leverantörer.

13.4. Leverantörer granskas med jämna mellanrum. Granskningens art, omfattning och frekvens beror på flera faktorer, bland annat vilken produkt/tjänst som tillhandahålls och hur kritisk leverantören är.

13.5. Kritiska leverantörers motståndskraft och återhämtningsförmåga granskas formellt på årsbasis som en del av vår Business Impact Analysis (BIA) av vår BC-återhämtningsförmåga.

## 14. KONTINUITET I VERKSAMHETEN OCH KATASTROFÅTERSTÄLLNING

14.1. I enlighet med vår ISO 22301-certifiering granskas kontinuitetsplanerna, inklusive Reed & Mackays krishanteringsplan, formellt varje år eller oftare om det behövs (t.ex. om det sker en betydande förändring).

14.2. Ett rullande program för kontinuitetsövningar och tester finns på plats, bestående av skrivbordsbaserade scenarioövningar och fysiska tester av återställningsplatser.

14.3. En årlig konsekvensanalys genomförs för att fastställa hur mycket störningar verksamheten kan tolerera i sina nyckelaktiviteter, vilken miniminivå av dessa aktiviteter som krävs för att verksamheten ska fungera samt vilka resurser och beroenden som krävs för att återuppta aktiviteterna

14.4. Reed & Mackays plattform för resehantering finns i Microsoft Azure, vilket ger hög grad av redundans och motståndskraft.

14.5. En online-backuptjänst från tredje part för att säkerställa att kritisk information som finns i virtuella maskiner och lagringskonton lagras säkert och oberoende av Azure-miljön och är tillgänglig för återställning i händelse av oavsiktlig förlust eller korruption.

14.6. Vår egen databas, inklusive all redovisnings-, kund- och rapporteringsdata, är föremål för en fullständig säkerhetskopiering dagligen och inkrementella säkerhetskopior under hela dagen. RPO är 1 timme och RTO är 3 timmar. Servrar säkerhetskopieras dagligen på en "inkrementell för alltid"-basis. RPO är 1 dag och RTO är 4 timmar. Vår övergripande RTO är 4 timmar.

14.7. Säkerhetskopiorna är krypterade och testas regelbundet.

## 15. RISK FÖR INFORMATIONSSÄKERHET

15.1. Riskbaserat tänkande och riskmedvetenhet ingår i Reed & Mackays ledningssystem och de processer som ligger till grund för det.

15.2. Programmet för hantering av informationssäkerhetsrisker är en del av företagets ramverk för riskhantering och omfattar identifiering och bedömning av informationssäkerhetsrisker som uppstår både genom olika återkommande aktiviteter och genom planerade och oplanerade förändringar. Identifierade risker prioriteras, behandlas/accepteras och godkänns i rätt tid.

15.3. Aktiviteter inom Reed & Mackays program för hantering av informationssäkerhet prioriteras utifrån identifierade risker och deras inverkan på de tjänster som tillhandahålls kunderna.

**Bilaga 3**

**Tillägg för Storbritannien**

**Tabell 1: Partier**

| | | |
|---|---|---|
| **Startdatum** | | |
| **Parterna** | **Exportör (som skickar den Begränsade överföringen)** | **Importör (som tar emot den Begränsade överföringen)** |
| **Uppgifter om parterna** | Enligt bilaga 1 i tillägget till EU:s SCC ovan | Enligt bilaga 1 i tillägget till EU:s SCC ovan |
| **Nyckelkontakt** | Enligt bilaga 1 i tillägget till EU:s SCC ovan | Enligt bilaga 1 i tillägget till EU:s SCC ovan |
| **Underskrift** | | |

**Tabell 2: Valda SCC, moduler och valda klausuler**

| | |
|---|---|
| **Addendum EU SCCs** | ☒ Den version av de Godkända EU SCC som detta Tillägg är bifogat till och som beskrivs nedan, inklusive Tilläggsinformationen:<br><br>Datum: |

**Tabell 3: Information om bilagor**

"**Tilläggsinformation**" avser den information som måste tillhandahållas för de valda modulerna enligt vad som anges i tillägget till de godkända EU SCC (andra än parterna), och som för detta tillägg anges i:

| |
|---|
| Bilaga 1A: Förteckning över parter: Tillägg av de godkända EU SCCs som anges i schemat. |
| Bilaga 1B: Beskrivning av överföringen: Tillägg till de Godkända EU SCCs som anges i Schemat. |
| Bilaga II: Tekniska och organisatoriska åtgärder, inklusive tekniska och organisatoriska åtgärder för att garantera datasäkerheten: Tillägg till de godkända EU SCC som anges i schemat. |
| Bilaga III: Förteckning över underprocessorer (endast modulerna 2 och 3): Tillägg till de godkända EU SCC som anges i schemat. |

**Tabell 4: Avsluta detta addendum när det godkända addendumet ändras**

| | |
|---|---|
| Avsluta detta tillägg när det godkända tillägget ändras | Vilka parter som kan avsluta detta tillägg enligt vad som anges i avsnitt 19:<br>☐ Importör<br>☒ Exportör<br>☐ inget parti |

| | |
|---|---|
| **Obligatoriska klausuler** | Del 2: Obligatoriska klausuler i det godkända tillägget, som är mallen Addendum B.1.0 som utfärdats av ICO och lagts fram för parlamentet i enlighet med s119A i dataskyddslagen 2018 den 2 februari 2022, såsom det revideras enligt avsnitt 18 i dessa obligatoriska klausuler. |