Umowa powierzenia przetwarzania danych osobowych

Szablon (bez klienta)

Wersja duńska jest prawnie wiążąca; niniejsze tłumaczenie ma charakter wyłącznie informacyjny.

Standardowe klauzule umowne na podstawie art. 28 ust. 3 rozporządzenia (UE) 2016/679 (ogólnego rozporządzenia o ochronie danych) do celów przetwarzania danych osobowych przez podmiot przetwarzający

Standardowa umowa Datatilsynet – duńskiego organu ochrony danych (styczeń 2020 r.) z załącznikami A–D Svarflow · Wersja 2026-11 · Obowiązuje od 19 listopada 2026 r.

pomiędzy

Administrator

[Pełna nazwa prawna administratora]

CVR [nr CVR]

[Adres]

[Kod pocztowy i miejscowość]

[Kraj]

zwanym dalej „administratorem”

Podmiot przetwarzający

Svarflow ApS

CVR 46871421

Dania

zwanym dalej „podmiotem przetwarzającym”

zwanymi dalej z osobna „stroną”, a łącznie „stronami”

UZGODNIŁY następujące standardowe klauzule umowne (zwane dalej „Klauzulami”) w celu zapewnienia zgodności z ogólnym rozporządzeniem o ochronie danych oraz ochrony prywatności i podstawowych praw i wolności osób fizycznych.

1. Spis treści

2. Preambuła
3. Prawa i obowiązki administratora
4. Podmiot przetwarzający działa na polecenie
5. Poufność
6. Bezpieczeństwo przetwarzania
7. Korzystanie z usług dalszych podmiotów przetwarzających
8. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych
9. Pomoc udzielana administratorowi

10. Zgłaszanie naruszeń ochrony danych osobowych
11. Usuwanie i zwrot danych
12. Audyt, w tym inspekcja
13. Uzgodnienia stron w innych kwestiach
14. Wejście w życie i rozwiązanie
15. Osoby kontaktowe administratora i podmiotu przetwarzającego
Załącznik A — Informacje o przetwarzaniu
Załącznik B — Dalsze podmioty przetwarzające
Załącznik C — Polecenia dotyczące przetwarzania danych osobowych
Załącznik D — Uregulowanie przez strony innych kwestii

2. Preambuła

2.1 Niniejsze Klauzule określają prawa i obowiązki podmiotu przetwarzającego w przypadku, gdy przetwarza on dane osobowe w imieniu administratora.

2.2 Niniejsze Klauzule zostały opracowane w celu zapewnienia przestrzegania przez strony art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej „RODO").

2.3 W związku ze świadczeniem usługi recepcjonistki telefonicznej AI Nora wraz z powiązanymi rezerwacjami, wiadomościami i potwierdzeniami SMS (zwanej dalej „Usługą") podmiot przetwarzający przetwarza dane osobowe w imieniu administratora zgodnie z niniejszymi Klauzulami.

2.4 Klauzule mają pierwszeństwo przed wszelkimi podobnymi postanowieniami zawartymi w innych umowach między stronami.

2.5 Do niniejszych Klauzul dołączone są cztery załączniki, które stanowią integralną część Klauzul.

2.6 Załącznik A zawiera szczegółowe informacje o przetwarzaniu danych osobowych, w tym o celu i charakterze przetwarzania, rodzaju danych osobowych, kategoriach osób, których dane dotyczą, oraz czasie trwania przetwarzania.

2.7 Załącznik B zawiera warunki administratora dotyczące korzystania przez podmiot przetwarzający z usług dalszych podmiotów przetwarzających oraz wykaz dalszych podmiotów przetwarzających, na których wykorzystanie administrator wyraził zgodę.

2.8 Załącznik C zawiera polecenia administratora dotyczące przetwarzania danych osobowych przez podmiot przetwarzający, opis środków bezpieczeństwa, które podmiot przetwarzający musi co najmniej wdrożyć, oraz opis sposobu sprawowania nadzoru nad podmiotem przetwarzającym i ewentualnymi dalszymi podmiotami przetwarzającymi.

2.9 Załącznik D zawiera postanowienia dotyczące innych czynności, które nie są objęte Klauzulami.

2.10 Klauzule wraz z załącznikami są przechowywane przez obie strony w formie pisemnej, w tym w formie elektronicznej.

2.11 Niniejsze Klauzule nie zwalniają podmiotu przetwarzającego z obowiązków nałożonych na niego na mocy RODO lub jakichkolwiek innych przepisów prawa.

3. Prawa i obowiązki administratora

3.1 Administrator odpowiada za zapewnienie, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO (zob. art. 24 RODO), przepisami o ochronie danych zawartymi w innych przepisach prawa Unii lub prawa krajowego państw członkowskich oraz z niniejszymi Klauzulami. Odniesienia do „państwa członkowskiego" w niniejszych Klauzulach należy rozumieć jako odniesienia do państw członkowskich EOG.

3.2 Administrator ma prawo i obowiązek podejmowania decyzji o celu (celach) i sposobach przetwarzania danych osobowych.

3.3 Administrator odpowiada między innymi za zapewnienie, aby istniała podstawa prawna przetwarzania danych osobowych, do którego wykonania podmiot przetwarzający otrzymuje polecenie.

4. Podmiot przetwarzający działa na polecenie

4.1 Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo krajowe państwa członkowskiego, któremu podlega podmiot przetwarzający. Polecenia te muszą być określone w załącznikach A i C. Administrator może również wydawać kolejne polecenia w trakcie przetwarzania danych osobowych, przy czym polecenia te muszą być zawsze udokumentowane i przechowywane w formie pisemnej, w tym elektronicznej, wraz z niniejszymi Klauzulami.

4.2 Podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane polecenie narusza RODO lub przepisy o ochronie danych zawarte w innych przepisach prawa Unii lub prawa krajowego państw członkowskich.

5. Poufność

5.1 Podmiot przetwarzający może udzielać dostępu do danych osobowych przetwarzanych w imieniu administratora wyłącznie osobom, które podlegają uprawnieniom podmiotu przetwarzającego do wydawania poleceń i które zobowiązały się do zachowania poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, i wyłącznie w niezbędnym zakresie. Wykaz osób, którym przyznano dostęp, podlega bieżącemu przeglądowi. Na podstawie tego przeglądu dostęp do danych osobowych może zostać cofnięty, jeżeli przestał być niezbędny, a dane osobowe nie mogą być wówczas dłużej dostępne dla tych osób.

5.2 Na wniosek administratora podmiot przetwarzający musi być w stanie wykazać, że osoby, które podlegają uprawnieniom podmiotu przetwarzającego do wydawania poleceń, podlegają wyżej wymienionemu obowiązkowi zachowania tajemnicy.

6. Bezpieczeństwo przetwarzania

6.1 Art. 32 RODO stanowi, że administrator i podmiot przetwarzający, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

6.2 Administrator ocenia ryzyko dla praw i wolności osób fizycznych, jakie wiąże się z przetwarzaniem, i wdraża środki zaradzające temu ryzyku. W zależności od ich adekwatności mogą one obejmować:

a) pseudonimizację i szyfrowanie danych osobowych

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

d) procedurę regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Zgodnie z art. 32 RODO podmiot przetwarzający – niezależnie od administratora – również ocenia ryzyko dla praw osób fizycznych, jakie wiąże się z przetwarzaniem, i wdraża środki zaradzające temu ryzyku. Na potrzeby tej oceny administrator udostępnia podmiotowi przetwarzającemu niezbędne informacje, które umożliwiają mu zidentyfikowanie i ocenę takiego ryzyka.

6.3 Ponadto podmiot przetwarzający pomaga administratorowi w wywiązaniu się z obowiązku administratora wynikającego z art. 32 RODO, między innymi poprzez udostępnienie administratorowi niezbędnych informacji dotyczących technicznych i organizacyjnych środków bezpieczeństwa, które podmiot przetwarzający już wdrożył zgodnie z art. 32 RODO, oraz wszelkich innych informacji niezbędnych do wywiązania się przez administratora z obowiązku wynikającego z art. 32 RODO.

6.4 Jeżeli zaradzenie zidentyfikowanemu ryzyku – w ocenie administratora – wymaga wdrożenia środków dodatkowych w stosunku do środków już wdrożonych przez podmiot przetwarzający, administrator określa w załączniku C dodatkowe środki, które należy wdrożyć.

7. Korzystanie z usług dalszych podmiotów przetwarzających

7.1 Podmiot przetwarzający spełnia warunki, o których mowa w art. 28 ust. 2 i 4 RODO, aby korzystać z usług innego podmiotu przetwarzającego (dalszego podmiotu przetwarzającego).

7.2 Podmiot przetwarzający nie może zatem korzystać z usług dalszego podmiotu przetwarzającego w celu wykonania niniejszych Klauzul bez uprzedniej ogólnej pisemnej zgody administratora.

7.3 Podmiot przetwarzający posiada ogólną zgodę administratora na korzystanie z usług dalszych podmiotów przetwarzających. Podmiot przetwarzający informuje administratora na piśmie o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających z co najmniej 30-dniowym wyprzedzeniem, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian przed skorzystaniem z usług danego dalszego podmiotu przetwarzającego (danych dalszych podmiotów przetwarzających). Dłuższy termin powiadomienia w odniesieniu do określonych czynności przetwarzania może zostać określony w załączniku B. Wykaz dalszych podmiotów przetwarzających, na których wykorzystanie administrator już wyraził zgodę, znajduje się w załączniku B.

7.4 Jeżeli podmiot przetwarzający korzysta z usług dalszego podmiotu przetwarzającego w celu wykonania w imieniu administratora określonych czynności przetwarzania, podmiot przetwarzający – na mocy umowy lub innego aktu prawnego zgodnie z prawem Unii lub prawem krajowym państwa członkowskiego – nakłada na dalszy podmiot przetwarzający te same obowiązki w zakresie ochrony danych, jakie wynikają z niniejszych Klauzul, przy czym w szczególności zapewnia się wystarczające gwarancje, że dalszy podmiot przetwarzający wdroży środki techniczne i organizacyjne w taki sposób, by przetwarzanie spełniało wymogi niniejszych Klauzul i RODO.

Podmiot przetwarzający odpowiada zatem za to, by wymagać od dalszego podmiotu przetwarzającego przestrzegania co najmniej obowiązków podmiotu przetwarzającego wynikających z niniejszych Klauzul i RODO.

7.5 Umowa (umowy) z dalszym podmiotem przetwarzającym oraz wszelkie późniejsze zmiany do niej (do nich) są przekazywane w kopii administratorowi – na jego wniosek – co daje mu możliwość upewnienia się, że na dalszy podmiot przetwarzający nałożono obowiązki w zakresie ochrony danych odpowiadające obowiązkom wynikającym z niniejszych Klauzul. Postanowień dotyczących warunków handlowych, które nie wpływają na treść umowy z dalszym podmiotem przetwarzającym w zakresie prawa ochrony danych, nie przekazuje się administratorowi.

7.6 Jeżeli dalszy podmiot przetwarzający nie wywiązuje się ze swoich obowiązków w zakresie ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków dalszego podmiotu przetwarzającego spoczywa nadal na podmiocie przetwarzającym. Nie narusza to praw osób, których dane dotyczą, wynikających z RODO, w szczególności z art. 79 i 82 RODO, wobec administratora i podmiotu przetwarzającego, w tym dalszego podmiotu przetwarzającego.

8. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych

8.1 Wszelkie przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych może być dokonywane przez podmiot przetwarzający wyłącznie na podstawie udokumentowanego polecenia administratora w tym zakresie i musi zawsze odbywać się zgodnie z rozdziałem V RODO.

8.2 Jeżeli przekazanie danych osobowych do państw trzecich lub organizacji międzynarodowych, do którego dokonania podmiot przetwarzający nie otrzymał polecenia od administratora, jest wymagane na mocy prawa Unii lub prawa krajowego państwa członkowskiego, któremu podlega podmiot przetwarzający, podmiot przetwarzający przed rozpoczęciem przetwarzania informuje administratora o tym obowiązku prawnym, chyba że prawo to zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

8.3 Bez udokumentowanego polecenia administratora podmiot przetwarzający nie może zatem w ramach niniejszych Klauzul:

a) przekazywać danych osobowych administratorowi lub podmiotowi przetwarzającemu w państwie trzecim lub w organizacji międzynarodowej

b) powierzać przetwarzania danych osobowych dalszemu podmiotowi przetwarzającemu w państwie trzecim

c) przetwarzać danych osobowych w państwie trzecim.

8.4 Polecenia administratora dotyczące przekazywania danych osobowych do państwa trzeciego, w tym ewentualna podstawa przekazania przewidziana w rozdziale V RODO, na której opiera się przekazanie, określa się w załączniku C.6.

8.5 Niniejszych Klauzul nie należy mylić ze standardowymi klauzulami umownymi, o których mowa w art. 46 ust. 2 lit. c) i d) RODO, a niniejsze Klauzule nie mogą stanowić podstawy przekazywania danych osobowych w rozumieniu rozdziału V RODO.

9. Pomoc udzielana administratorowi

9.1 Podmiot przetwarzający, uwzględniając charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich

praw określonych w rozdziale III RODO.

Oznacza to, że podmiot przetwarzający w miarę możliwości pomaga administratorowi w zapewnieniu przez administratora przestrzegania:

a) obowiązku informacyjnego w przypadku zbierania danych osobowych od osoby, której dane dotyczą

b) obowiązku informacyjnego w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

c) prawa dostępu

d) prawa do sprostowania danych

e) prawa do usunięcia danych („prawa do bycia zapomnianym")

f) prawa do ograniczenia przetwarzania

g) obowiązku powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

h) prawa do przenoszenia danych

i) prawa do sprzeciwu

j) prawa do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

9.2 Oprócz obowiązku podmiotu przetwarzającego do udzielania pomocy administratorowi zgodnie z klauzulą 6.3 podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga ponadto administratorowi w wywiązaniu się z:

a) obowiązku administratora do zgłoszenia naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu – w przypadku administratora w Danii: Datatilsynet – bez zbędnej zwłoki i w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych

b) obowiązku administratora do zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych

c) obowiązku administratora do dokonania przed rozpoczęciem przetwarzania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (oceny skutków)

d) obowiązku administratora do konsultacji z właściwym organem nadzorczym – w przypadku administratora w Danii: Datatilsynet – przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka.

9.3 Strony określają w załączniku C odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający ma pomagać administratorowi, a także ich zakres i zasięg. Dotyczy to obowiązków wynikających z klauzul 9.1 i 9.2.

10. Zgłaszanie naruszeń ochrony danych osobowych

10.1 Po stwierdzeniu naruszenia ochrony danych osobowych podmiot przetwarzający bez zbędnej zwłoki powiadamia o nim administratora.

10.2 Powiadomienie przekazywane przez podmiot przetwarzający administratorowi następuje w miarę możliwości nie później niż w terminie 24 godzin od stwierdzenia przez niego naruszenia, tak aby administrator mógł wywiązać się z obowiązku zgłoszenia naruszenia ochrony danych

osobowych właściwemu organowi nadzorczemu, zgodnie z art. 33 RODO.

10.3 Zgodnie z klauzulą 9.2 lit. a) podmiot przetwarzający pomaga administratorowi w dokonaniu zgłoszenia naruszenia właściwemu organowi nadzorczemu. Oznacza to, że podmiot przetwarzający pomaga w dostarczeniu poniższych informacji, które zgodnie z art. 33 ust. 3 muszą być zawarte w zgłoszeniu naruszenia dokonywanym przez administratora właściwemu organowi nadzorczemu:

a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie

b) możliwe konsekwencje naruszenia ochrony danych osobowych

c) środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

10.4 Strony określają w załączniku C informacje, które podmiot przetwarzający ma dostarczyć w ramach pomocy udzielanej administratorowi w wywiązaniu się przez niego z obowiązku zgłaszania naruszeń ochrony danych osobowych właściwemu organowi nadzorczemu.

11. Usuwanie i zwrot danych

11.1 Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych podmiot przetwarzający jest zobowiązany usunąć wszelkie dane osobowe przetwarzane w imieniu administratora i potwierdzić administratorowi, że dane zostały usunięte – chyba że administrator najpóźniej w chwili zakończenia wybrał na piśmie ich zwrot, w którym to przypadku podmiot przetwarzający zwraca wszystkie dane osobowe i usuwa istniejące kopie – chyba że prawo Unii lub prawo krajowe państwa członkowskiego nakazuje przechowywanie danych osobowych. Termin i sposób postępowania określono w załączniku C.4.

11.2 Żadne przepisy prawa Unii ani prawa duńskiego nie nakazują przechowywania danych osobowych, które podmiot przetwarzający przetwarza w imieniu administratora, po zakończeniu świadczenia usług.

12. Audyt, w tym inspekcja

12.1 Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania przestrzegania art. 28 RODO i niniejszych Klauzul oraz umożliwia administratorowi lub innemu audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

12.2 Procedury audytów, w tym inspekcji, przeprowadzanych przez administratora u podmiotu przetwarzającego i dalszych podmiotów przetwarzających określono szczegółowo w załącznikach C.7 i C.8.

12.3 Podmiot przetwarzający jest zobowiązany zapewnić organom nadzorczym, które zgodnie z obowiązującymi przepisami mają dostęp do pomieszczeń administratora lub podmiotu przetwarzającego, lub przedstawicielom działającym w imieniu organu nadzorczego, dostęp do fizycznych pomieszczeń podmiotu przetwarzającego za okazaniem odpowiedniej legitymacji.

13. Uzgodnienia stron w innych kwestiach

13.1 Strony mogą uzgodnić inne postanowienia dotyczące usługi przetwarzania danych osobowych, np. w zakresie odpowiedzialności odszkodowawczej, o ile te inne postanowienia nie są bezpośrednio ani pośrednio sprzeczne z Klauzulami ani nie ograniczają podstawowych praw i

wolności osoby, której dane dotyczą, wynikających z RODO.

14. Wejście w życie i rozwiązanie

14.1 Klauzule wchodzą w życie z dniem ich podpisania przez obie strony. Podpis może zostać złożony elektronicznie w procesie konfiguracji Svarflow (rejestrowane są imię i nazwisko, stanowisko, czas oraz wersja umowy), zgodnie z art. 28 ust. 9 RODO.

14.2 Każda ze stron może zażądać renegocjacji Klauzul, jeżeli uzasadniają to zmiany przepisów prawa lub nieadekwatność Klauzul.

14.3 Klauzule obowiązują przez cały okres świadczenia usługi przetwarzania danych osobowych. W tym okresie Klauzule nie mogą zostać wypowiedziane, chyba że strony uzgodnią inne postanowienia regulujące świadczenie usługi przetwarzania danych osobowych.

14.4 Jeżeli świadczenie usług przetwarzania danych osobowych zostanie zakończone, a dane osobowe zostaną usunięte lub zwrócone administratorowi zgodnie z klauzulą 11.1 i załącznikiem C.4, Klauzule mogą zostać wypowiedziane przez każdą ze stron w drodze pisemnego wypowiedzenia.

Podpis

W imieniu administratora

Imię i nazwisko	[Imię i nazwisko]
Stanowisko	[Stanowisko]
Numer telefonu	[Numer telefonu]
E-mail	[E-mail]
Data i podpis	

W imieniu podmiotu przetwarzającego

Imię i nazwisko	Jesper Rune Thomasen
Stanowisko	Dyrektor zarządzający, Svarflow ApS
Numer telefonu	+45 35 15 47 47
E-mail	legal@svarflow.dk
Data i podpis	

15. Osoby kontaktowe administratora i podmiotu przetwarzającego

15.1 Strony mogą kontaktować się ze sobą za pośrednictwem wskazanych poniżej osób kontaktowych.

15.2 Strony są zobowiązane do bieżącego informowania się nawzajem o zmianach dotyczących osób kontaktowych.

Osoba kontaktowa administratora

Imię i nazwisko	[Imię i nazwisko]
Stanowisko	[Stanowisko]
Numer telefonu	[Numer telefonu]

E-mail	[E-mail]

Osoba kontaktowa podmiotu przetwarzającego

Imię i nazwisko	Jesper Rune Thomasen
Stanowisko	Dyrektor zarządzający
Numer telefonu	+45 35 15 47 47
E-mail	legal@svarflow.dk (sprawy dotyczące danych osobowych, praw osób, których dane dotyczą, oraz incydentów bezpieczeństwa)

Załącznik A — Informacje o przetwarzaniu

A.1. Cel przetwarzania danych osobowych przez podmiot przetwarzający w imieniu administratora

Podmiot przetwarzający odbiera połączenia telefoniczne kierowane do przedsiębiorstwa administratora za pomocą recepcjonistki telefonicznej AI Nora i wykonuje w imieniu administratora:

- odbieranie połączeń przychodzących na numer telefonu administratora,
- rezerwowanie, przesuwanie i odwoływanie wizyt we własnym kalendarzu lub systemie rezerwacji administratora zgodnie z regułami administratora,
- przekazywanie administratorowi wiadomości o tym, czego życzy sobie osoba dzwoniąca,
- potwierdzenia SMS dla osoby dzwoniącej (osoba dzwoniąca sama potwierdza wizytę, zanim zacznie ona obowiązywać),
- przekierowywanie połączeń na własny numer administratora, jeżeli administrator wybrał taką opcję.

A.2. Przetwarzanie danych osobowych przez podmiot przetwarzający w imieniu administratora dotyczy przede wszystkim (charakter przetwarzania)

Odbierania połączenia, zamiany mowy na tekst, prowadzenia rozmowy z osobą dzwoniącą za pomocą modelu językowego, podsumowywania, przechowywania i przekazywania administratorowi treści rozmowy – a także nagrywania dźwięku, jeżeli administrator wybrał taką opcję (reguła „Zapisuj dźwięk rozmów” w panelu administracyjnym Svarflow; domyślnie wyłączona) – oraz tworzenia, zmieniania i odwoływania wizyt w kalendarzu administratora.

A.3. Przetwarzanie obejmuje następujące rodzaje danych osobowych osób, których dane dotyczą

- imię i nazwisko
- numer telefonu
- adres e-mail, jeżeli osoba dzwoniąca go poda
- godzina połączenia i czas jego trwania
- treść rozmowy: transkrypcja i podsumowanie – oraz nagranie dźwięku, jeżeli administrator wybrał taką opcję (reguła „Zapisuj dźwięk rozmów”; domyślnie wyłączona)
- dane dotyczące rezerwacji: czego dotyczy wizyta, kiedy i u kogo się odbywa, a także uwagi osoby dzwoniącej dotyczące wizyty

Szczególne kategorie danych osobowych (art. 9). U administratorów z sektora ochrony zdrowia i podobnych w treści rozmowy mogą pojawiać się dane dotyczące zdrowia, ponieważ osoba dzwoniąca sama je przekazuje. Nora nigdy nie pyta o dane dotyczące zdrowia, numery ewidencyjne (CPR) ani dane płatnicze – jest to stałe polecenie – a jeżeli osoba dzwoniąca mimo to je poda, Nora ich nie

powtarza ani nie notuje. Mogą one jednak znaleźć się w transkrypcji rozmowy oraz w nagraniu dźwięku, jeżeli administrator włączył nagrywanie. Administrator musi zatem ocenić, czy przetwarzanie u danego administratora obejmuje dane, o których mowa w art. 9, i zapewnić podstawę prawną ich przetwarzania.

A.4. Przetwarzanie obejmuje następujące kategorie osób, których dane dotyczą

Klienci, pacjenci, zleceniodawcy lub goście administratora – czyli osoby, które dzwonią na numer telefonu administratora, oraz osoby, dla których umawiana jest wizyta. Ponadto pracownicy administratora w zakresie, w jakim występują jako osoba świadcząca usługę lub osoba kontaktowa w ramach wizyty.

A.5. Przetwarzanie danych osobowych przez podmiot przetwarzający w imieniu administratora może rozpocząć się po wejściu w życie niniejszych Klauzul. Przetwarzanie trwa przez następujący okres

Przetwarzanie trwa tak długo, jak obowiązuje zawarta między stronami umowa abonamentowa dotycząca Usługi. Po jej zakończeniu dane osobowe są usuwane lub zwracane, według wyboru administratora, w terminie 90 dni, zgodnie z klauzulą 11.1 i załącznikiem C.4.

Załącznik B — Dalsze podmioty przetwarzające

B.1. Zatwierdzone dalsze podmioty przetwarzające

W chwili wejścia w życie Klauzul administrator wyraził zgodę na korzystanie z usług następujących dalszych podmiotów przetwarzających:

Dalszy podmiot przetwarzający	Rola w przetwarzaniu	Państwo / miejsce przetwarzania	Podstawa przekazania
Telnyx LLC	Telefonia: odbiera połączenie na numer administratora i łączy je z Norą	USA	Standardowe klauzule umowne Komisji Europejskiej (2021/914) zawarte w umowie powierzenia przetwarzania danych Telnyx; Telnyx jest ponadto certyfikowany zgodnie z ramami ochrony danych UE–USA (EU-U.S. Data Privacy Framework)
ElevenLabs, Inc.	Zamiana mowy na tekst, głos Nory i AI do prowadzenia rozmów; model językowy w rozmowie jest wywoływany za pośrednictwem ElevenLabs. Dźwięk i transkrypcja są usuwane w ElevenLabs po 30 dniach	USA	Standardowe klauzule umowne (2021/914) zawarte w umowie powierzenia przetwarzania danych ElevenLabs; ElevenLabs jest ponadto certyfikowany zgodnie z ramami ochrony danych UE–USA (EU-U.S. Data Privacy Framework)
Anthropic, PBC	Model językowy w rozmowie (za pośrednictwem ElevenLabs) oraz analiza rozmów: podsumowanie, wiadomość dla administratora, pomiar jakości	USA	Standardowe klauzule umowne (2021/914, moduł 2 i 3) zawarte w umowie powierzenia przetwarzania danych Anthropic. Dane klientów nie są wykorzystywane do trenowania modeli
Vercel Inc.	Obsługa działania oprogramowania Svarflow (funkcje serwerowe)	USA; funkcje są wykonywane we Frankfurcie, Niemcy (region fra1)	Standardowe klauzule umowne (2021/914) zawarte w umowie powierzenia przetwarzania danych Vercel

Supabase Pte. Ltd	Baza danych, pliki (w tym nagrania dźwięku) i logowanie	Singapur; baza danych i pliki znajdują się we Frankfurcie, Niemcy (AWS eu-central-1)	Standardowe klauzule umowne (2021/914, moduł 2 i 3) zawarte w umowie powierzenia przetwarzania danych Supabase
ONLINECITY.IO ApS (GatewayAPI), nr CVR 27364276	SMS do osób, których dane dotyczą (potwierdzenia i wiadomości)	Dania; hosting w Hetzner Online GmbH, Niemcy (konfiguracja w UE)	Brak przekazywania do państwa trzeciego
Simply.com A/S	Wychodząca poczta e-mail do administratora (wiadomości i powiadomienia)	Dania	Brak przekazywania do państwa trzeciego
Hetzner Online GmbH	Serwer integracyjny Svarflow łączący z systemem rezerwacji administratora (konektor chmurowy)	Niemcy (Falkenstein)	Brak przekazywania do państwa trzeciego

Własni dostawcy administratora. Jeżeli administrator korzysta z Kalendarza Google lub innego systemu rezerwacji, Svarflow wpisuje wizyty na własne konto administratora u danego dostawcy. Dostawca przetwarza wówczas dane na podstawie własnej umowy administratora z tym dostawcą i nie jest dalszym podmiotem przetwarzającym Svarflow.

Konfiguracja. Podczas konfiguracji Svarflow odczytuje publiczną stronę internetową administratora za pośrednictwem usługi Firecrawl (SideGuide Technologies, Inc., USA), aby poznać usługi i godziny otwarcia przedsiębiorstwa. Do tej usługi nie są przesyłane żadne informacje o osobach, których dane dotyczą.

W chwili wejścia w życie Klauzul administrator wyraził zgodę na korzystanie z usług wyżej wymienionych dalszych podmiotów przetwarzających w odniesieniu do opisanej czynności przetwarzania. Podmiot przetwarzający nie może – bez pisemnej zgody administratora – korzystać z usług dalszego podmiotu przetwarzającego w odniesieniu do czynności przetwarzania innej niż opisana i uzgodniona ani korzystać z usług innego dalszego podmiotu przetwarzającego w odniesieniu do tej czynności przetwarzania.

B.2. Termin powiadomienia w sprawie zatwierdzania dalszych podmiotów przetwarzających

Podmiot przetwarzający powiadamia administratora na piśmie (pocztą elektroniczną na adres osoby kontaktowej administratora) z co najmniej 30-dniowym wyprzedzeniem przed dodaniem lub zastąpieniem dalszego podmiotu przetwarzającego. Administrator może wyrazić sprzeciw przed upływem tego terminu. Jeżeli strony nie osiągną porozumienia w sprawie sprzeciwu, administrator może wypowiedzieć Usługę ze skutkiem od chwili, w której nowy dalszy podmiot przetwarzający zostanie wykorzystany. Aktualny wykaz dalszych podmiotów przetwarzających jest dostępny na stronie svarflow.dk.

Załącznik C — Polecenia dotyczące przetwarzania danych osobowych

C.1. Przedmiot przetwarzania / polecenia

Przetwarzanie danych osobowych przez podmiot przetwarzający w imieniu administratora polega na wykonywaniu przez podmiot przetwarzający następujących czynności:

- odbieranie połączeń na numer administratora za pomocą recepcjonistki telefonicznej AI Nora,
- tworzenie, przesuwanie i odwoływanie wizyt w kalendarzu lub systemie rezerwacji administratora zgodnie z regułami rezerwacji administratora – wizyta obowiązuje dopiero wtedy, gdy osoba

dzwoniąca sama potwierdzi ją za pośrednictwem SMS,

- przyjmowanie wiadomości dla administratora i przekazywanie ich pocztą elektroniczną, SMS-em lub w panelu administracyjnym Svarflow,
- wysyłanie potwierdzeń SMS do osoby dzwoniącej,
- podawanie własnego numeru dyżurnego administratora lub przekierowywanie połączeń zgodnie z poleceniem administratora.

Administrator sam zarządza regułami – godzinami otwarcia, regułami rezerwacji, powitaniem, poleceniami na wypadek pilnych spraw, tym, czy można nagrywać dźwięk, jak długo przechowywane są rozmowy i kiedy Nora ma przyjąć wiadomość – w panelu administracyjnym Svarflow. Zmiany w tym zakresie stanowią udokumentowane polecenia, zgodnie z klauzulą 4.1.

Nora nie udziela porad medycznych, nie ocenia objawów i nie podejmuje żadnych decyzji dotyczących osoby, której dane dotyczą. Nora informuje w powitaniu, że osoba dzwoniąca rozmawia z asystentem AI.

Nagrywanie dźwięku odbywa się wyłącznie wtedy, gdy administrator wybrał taką opcję (reguła „Zapisuj dźwięk rozmów"), w celu udokumentowania tego, co zostało powiedziane i uzgodnione – transkrypcja może być błędna, a zatem potrzeby tej nie można zaspokoić w inny sposób (wytyczne Datatilsynet dotyczące nagrywania rozmów telefonicznych, kwiecień 2024 r.). Osoba dzwoniąca jest informowana w powitaniu o nagrywaniu i jego celu.

C.2. Bezpieczeństwo przetwarzania

Poziom bezpieczeństwa musi uwzględniać:

- fakt, że przetwarzane są zwykłe dane osobowe osób, których dane dotyczą (imię i nazwisko, numer telefonu, treść rozmów i wizyty),
- fakt, że u administratorów z sektora ochrony zdrowia w treści rozmowy mogą pojawiać się dane dotyczące zdrowia, ponieważ osoba dzwoniąca sama je przekazuje (załącznik A.3), oraz
- fakt, że treść rozmowy jest przetwarzana w postaci jawnego tekstu przez dalsze podmioty przetwarzające w USA, aby Nora mogła ją zrozumieć i odpowiedzieć (załącznik C.6).

Podmiot przetwarzający jest w związku z tym uprawniony i zobowiązany do podejmowania decyzji o tym, jakie techniczne i organizacyjne środki bezpieczeństwa należy wdrożyć, aby zapewnić niezbędny (i uzgodniony) poziom bezpieczeństwa.

Podmiot przetwarzający musi jednak – w każdym przypadku i co najmniej – wdrożyć następujące środki uzgodnione z administratorem:

- Szyfrowanie podczas przesyłania: cała komunikacja między oprogramowaniem Svarflow, osobami, których dane dotyczą, a dalszymi podmiotami przetwarzającymi odbywa się z wykorzystaniem protokołu TLS.
- Szyfrowanie w spoczynku: dane są szyfrowane w spoczynku u dalszych podmiotów przetwarzających (baza danych, pliki i nagrania dźwięku).
- Dane logowania administratora do systemu rezerwacji: gdy Svarflow łączy się z systemem rezerwacji administratora przy użyciu własnego dostępu administratora, dane logowania są szyfrowane kluczem, który może odszyfrować wyłącznie serwer integracyjny w UE (X25519 i AES-256-GCM). Ani funkcje serwerowe Svarflow, ani baza danych nie mogą ich odczytać, a dane te są usuwane, gdy administrator odłączy połączenie.
- Zarządzanie kluczami: klucze produkcyjne są przechowywane wyłącznie w zaszyfrowanej konfiguracji środowiska u dostawcy infrastruktury i nigdy nie są udostępniane w postaci jawnego tekstu, w kodzie źródłowym ani w plikach dziennika.
- Kontrola dostępu: dostęp do panelu administracyjnego Svarflow wymaga osobistego logowania;

funkcje przeznaczone dla pracowników Svarflow są dostępne wyłącznie dla zatwierdzonych kont. Wykaz osób posiadających dostęp podlega bieżącemu przeglądowi zgodnie z klauzulą 5.1.

- Dostęp przez internet: dostęp administratora do własnych danych odbywa się z wykorzystaniem protokołu TLS po osobistym zalogowaniu; baza danych zezwala wyłącznie na te odczyty i zapisy, do których uprawniona jest dana rola (kontrola dostępu na poziomie wierszy).
- Kontrola zmian: każda zmiana w systemie jest sprawdzana przez automatyczne testy blokujące, które wszystkie muszą zakończyć się wynikiem pozytywnym (zielonym), zanim zmiana będzie mogła zostać wdrożona.
- Rejestrowanie zdarzeń: dzienniki systemowe zawierają krótkie identyfikatory, znaczniki czasu i zamaskowane numery telefonów – nie zawierają treści rozmów ani pełnych danych osobowych.
- Minimalizacja danych u źródła: polecenia dla Nory pozwalają prosić wyłącznie o to, czego wymaga zadanie – zazwyczaj o imię i nazwisko oraz numer telefonu komórkowego – i zakazują proszenia o numer ewidencyjny (CPR), dane karty płatniczej, numery rachunków, hasła i szczegółowe informacje dotyczące zdrowia.
- Potwierdzenie przez osobę, której dane dotyczą: nic, co Nora uzgodni, nie zostaje wpisane do kalendarza administratora, zanim osoba dzwoniąca sama tego nie potwierdzi za pomocą linku w wiadomości SMS. Link wygasa po 24 godzinach.
- Ograniczone przechowywanie u dalszego podmiotu przetwarzającego: ElevenLabs przechowuje dźwięk i transkrypcję przez 30 dni, po czym są one usuwane. Dźwięk jest nagrywany wyłącznie wtedy, gdy administrator wybrał taką opcję.
- Zrzuty ekranu błędów z serwera integracyjnego: nigdy nie są wykonywane na etapie logowania, są przechowywane z ograniczonymi uprawnieniami, bez danych osobowych w nazwie pliku, i są automatycznie usuwane po 72 godzinach.
- Oddzielenie środowiska testowego od produkcyjnego: dane testowe nigdy nie są tworzone z wykorzystaniem prawdziwych danych identyfikacyjnych.
- Regularne testowanie: środki bezpieczeństwa są poddawane przeglądowi co najmniej raz w roku oraz w przypadku istotnych zmian w systemie lub u dalszych podmiotów przetwarzających; przegląd jest dokumentowany.

Opisane środki są środkami faktycznie wdrożonymi. Podmiot przetwarzający nie posiada certyfikatu ISO 27001, nie posiada raportu SOC 2 i nie zlecił przeprowadzenia zewnętrznego testu bezpieczeństwa przez stronę trzecią. Informuje się o tym otwarcie, aby administrator mógł ocenić, czy należy uzgodnić dodatkowe środki, zgodnie z klauzulą 6.4.

C.3. Pomoc udzielana administratorowi

Podmiot przetwarzający w miarę możliwości – w określonym poniżej zakresie i zasięgu – pomaga administratorowi zgodnie z klauzulami 9.1 i 9.2, wdrażając następujące środki techniczne i organizacyjne:

- Prawa osób, których dane dotyczą (art. 15–22): podmiot przetwarzający wyszukuje i udostępnia dane przetwarzane na temat osoby, której dane dotyczą (rozmowy, wizyty i wiadomości), oraz usuwa je lub dokonuje ich sprostowania zgodnie z poleceniem administratora. Żądania należy kierować na adres legal@svarflow.dk; odpowiedź udzielana jest nie później niż w terminie 10 dni roboczych od ich otrzymania, aby administrator mógł dotrzymać własnego terminu jednego miesiąca.
- Bezpieczeństwo przetwarzania (art. 32): poprzez utrzymywanie środków określonych w C.2 i udzielanie o nich informacji na żądanie.
- Naruszenie ochrony danych osobowych (art. 33–34): poprzez powiadomienie administratora w terminie określonym w klauzuli 10.2 i dostarczenie informacji, o których mowa w klauzuli 10.3:

charakteru incydentu, czasu jego wystąpienia i czasu jego wykrycia, rodzajów danych, których dotyczy, i przybliżonej liczby osób, których dane dotyczą, możliwych konsekwencji, środków podjętych przez podmiot przetwarzający oraz zalecenia podmiotu przetwarzającego w sprawie zgłoszenia i zawiadomienia. Powiadomienie jest przesyłane pocztą elektroniczną do osoby kontaktowej administratora i uzupełniane w miarę uzyskiwania przez podmiot przetwarzający dalszych informacji.

- Ocena skutków dla ochrony danych i uprzednie konsultacje (art. 35–36): podmiot przetwarzający udostępnia niniejszy załącznik, wykaz dalszych podmiotów przetwarzających, ocenę przekazania danych oraz inną niezbędną dokumentację.

C.4. Okres przechowywania / procedura usuwania

Dane	Przechowywanie i usuwanie
Dane osobowe w rezerwacji (kolejka zleceń)	Usuwane automatycznie po zrealizowaniu zlecenia
Karta oczekująca (wizyta oczekująca na potwierdzenie przez osobę dzwoniącą)	Wygasa po 24 godzinach bez potwierdzenia; usuwana automatycznie najpóźniej po 7 dniach
Transkrypcja i podsumowanie	Wybór administratora: 30, 90 (domyślnie) lub 180 dni
Nagranie dźwięku (wyłącznie przy regule „Zapisuj dźwięk rozmów” – wybór administratora, domyślnie wyłączona)	Wybór administratora: 30, 90 (domyślnie) lub 180 dni
Dźwięk i transkrypcja w ElevenLabs (dalszy podmiot przetwarzający)	Usuwane automatycznie po 30 dniach
Wiadomości dla administratora	Przez okres trwania abonamentu; po jego zakończeniu usuwane zgodnie z poniższymi zasadami
Po zakończeniu umowy	Wszystkie dane osobowe są usuwane lub zwracane, według wyboru administratora, w terminie 90 dni, po czym podmiot przetwarzający potwierdza usunięcie na piśmie

Terminy dotyczące kolejki zleceń, kart oczekujących, transkrypcji, podsumowań i nagrań dźwięku są egzekwowane automatycznie przez system: codzienne zadanie usuwa dane osobowe z rozmowy, kasuje plik dźwiękowy i pozostawia wyłącznie to, co jest niezbędne do działania systemu (identyfikator rozmowy, czas trwania i wynik). Administrator sam wybiera termin – 30, 90 lub 180 dni – w panelu administracyjnym Svarflow; w przypadku wybrania krótszego terminu starsze rozmowy są usuwane podczas najbliższego nocnego przebiegu. Usunięcia po zakończeniu umowy dokonuje podmiot przetwarzający według wyboru administratora, zgodnie z klauzulą 11.1.

Po zakończeniu świadczenia usługi przetwarzania danych osobowych podmiot przetwarzający usuwa albo zwraca dane osobowe zgodnie z klauzulą 11.1, chyba że administrator – po podpisaniu niniejszych Klauzul – zmienił swój pierwotny wybór. Takie zmiany muszą być udokumentowane i przechowywane w formie pisemnej, w tym elektronicznej, w powiązaniu z Klauzulami.

C.5. Miejsce przetwarzania

Przetwarzanie danych osobowych objętych Klauzulami nie może bez uprzedniej pisemnej zgody administratora odbywać się w innych miejscach niż następujące:

- Frankfurt, Niemcy (UE): własne oprogramowanie Svarflow (Vercel, region fra1) oraz baza danych z plikami i nagraniami dźwięku (Supabase, AWS eu-central-1).

- Falkenstein, Niemcy (UE): serwer integracyjny Svarflow (Hetzner) oraz hosting wysyłki SMS (GatewayAPI).
- Dania: wychodząca poczta e-mail (Simply.com).
- USA: telefonia (Telnyx), zamiana mowy na tekst, głos i AI do prowadzenia rozmów (ElevenLabs) oraz model językowy i analiza rozmów (Anthropic).
- Singapur: podmiot Supabase będący stroną umowy; sama baza danych znajduje się we Frankfurcie.

C.6. Polecenia dotyczące przekazywania danych osobowych do państw trzecich

Administrator poleca podmiotowi przetwarzającemu przekazywanie danych osobowych do dalszych podmiotów przetwarzających w USA i Singapurze wskazanych w załączniku B, na podstawie przekazania wskazanej przy każdym z nich: standardowych klauzul umownych Komisji Europejskiej (decyzja wykonawcza (UE) 2021/914, art. 46 ust. 2 lit. c) RODO), które stanowią część umowy powierzenia przetwarzania danych każdego z dostawców. Jeżeli dostawca jest ponadto certyfikowany zgodnie z ramami ochrony danych UE–USA (EU-U.S. Data Privacy Framework), przekazanie opiera się również na decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony z dnia 10 lipca 2023 r. (art. 45); standardowe klauzule umowne mają zastosowanie niezależnie od tego.

Przekazanie jest niezbędne do świadczenia Usługi: rozmowa musi być przetwarzana w postaci jawnego tekstu, aby Nora mogła ją zrozumieć i odpowiedzieć, a przed przekazaniem nie usuwa się z niej żadnych danych. Podmiot przetwarzający dokonał oceny przekazań (ocena przekazania danych) i udostępnia ją administratorowi na żądanie. Podmiot przetwarzający dokonuje ponownej weryfikacji podstawy przekazania, jeżeli decyzja stwierdzająca odpowiedni stopień ochrony zostanie uchylona lub zawieszona, i powiadamia administratora, jeżeli zmienia to podstawę przekazania w odniesieniu do któregokolwiek dalszego podmiotu przetwarzającego.

Jeżeli administrator nie wyda w niniejszych Klauzulach lub w terminie późniejszym udokumentowanego polecenia dotyczącego przekazywania danych osobowych do państwa trzeciego, podmiot przetwarzający nie jest uprawniony do dokonywania takich przekazań w ramach niniejszych Klauzul.

C.7. Procedury audytów, w tym inspekcji, przeprowadzanych przez administratora w odniesieniu do przetwarzania danych osobowych powierzonego podmiotowi przetwarzającemu

Administrator lub przedstawiciel administratora może raz w roku – a ponadto w przypadku wystąpienia naruszenia ochrony danych osobowych lub gdy wymaga tego organ nadzorczy – przeprowadzić audyt, w tym inspekcję, przetwarzania danych osobowych przez podmiot przetwarzający. O audycie zawiadamia się na piśmie z co najmniej 30-dniowym wyprzedzeniem, chyba że jest on spowodowany naruszeniem. Podmiot przetwarzający udostępnia niezbędną dokumentację: niniejszy załącznik, wykaz dalszych podmiotów przetwarzających i zawartych z nimi umów powierzenia przetwarzania danych (zgodnie z klauzulą 7.5), opis środków technicznych i organizacyjnych zawarty w C.2, ocenę przekazania danych, procedurę postępowania w przypadku naruszenia ochrony danych oraz rejestr czynności przetwarzania.

Podmiot przetwarzający nie pozyskuje sprawozdań z audytu od niezależnych stron trzecich (np. ISAE 3000). Ewentualne koszty administratora związane z audytem ponosi sam administrator. Podmiot przetwarzający jest jednak zobowiązany do przeznaczenia zasobów (głównie czasu) niezbędnych do przeprowadzenia przez administratora audytu. Na podstawie wyników administrator jest uprawniony do żądania wdrożenia dodatkowych środków w celu zapewnienia zgodności z RODO i niniejszymi Klauzulami.

C.8. Procedury audytów, w tym inspekcji, w odniesieniu do przetwarzania danych osobowych powierzonego dalszym podmiotom przetwarzającym

Dalsze podmioty przetwarzające dokumentują swoje bezpieczeństwo za pomocą niezależnych raportów z audytu i certyfikatów (np. SOC 2, ISO 27001 lub ISAE 3000). Podmiot przetwarzający pozyskuje je i dokonuje ich przeglądu co najmniej raz w roku, a w każdym przypadku wtedy, gdy dalszy podmiot przetwarzający istotnie zmieni sposób przetwarzania lub dotknie go naruszenie. Dokumentacja jest udostępniana administratorowi na żądanie. Podmiot przetwarzający nie przeprowadza fizycznych inspekcji u dalszych podmiotów przetwarzających. Na podstawie wyników administrator jest uprawniony do żądania wdrożenia dodatkowych środków, a ponadto może wyrazić sprzeciw wobec dalszego podmiotu przetwarzającego zgodnie z załącznikiem B.2.

Załącznik D — Uregulowanie przez strony innych kwestii

Uzgodnienia stron dotyczące odpowiedzialności odszkodowawczej wynikają z umowy abonamentowej dotyczącej Usługi w zakresie, w jakim nie są one bezpośrednio ani pośrednio sprzeczne z Klauzulami ani nie ograniczają praw osób, których dane dotyczą, zgodnie z klauzulą 13.1. Poza tym strony nie uzgodniły odrębnych postanowień.

Dokument opiera się na standardowych klauzulach umownych Datatilsynet (styczeń 2020 r.), w sprawie których Europejska Rada Ochrony Danych wydała opinię (opinia 14/2019). Klauzule 2–15 stanowią tekst standardowej umowy z uzupełnionymi wyborami stron; załączniki A–D pochodzą od Svarflow. W przypadku rozbieżności między tłumaczeniem a tekstem duńskim rozstrzygający jest tekst duński.