ZARZĄDZENIE NR 139/2019
BURMISTRZA MIASTA I GMINY CHMIELNIK
z dnia 15 listopada 2019 r.

w sprawie regulaminu Biuletynu Informacji Publicznej Urzędu Miasta i Gminy w Chmielniku

Na podstawie art.33 ust.1,3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j Dz.U. 2019 r., poz. 506) oraz art.4 ust.1 pkt 1 i art.8 ust.2 i 3 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2019 r. poz. 1429) oraz § 15 ust.1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 roku w sprawie Biuletynu Informacji Publicznej (Dz.U. z 2007 r. nr 10, poz. 68) zarządzam, co następuje:

§ 1. Wyznaczam do funkcji administratorów strony podmiotowej Biuletynu Informacji Publicznej Urzędu Miasta i Miasta w Chmielniku, zwany dalej BIP, pracowników Urzędu: Tomasza Biernackiego i Damiana Tomaszewskiego.

§ 2. 1. Powołuję zespół redakcyjny BIP, w skład którego wchodzą:
1) Administratorzy strony podmiotowej Biuletynu Informacji Publicznej.
2) Pracownicy wydziałów Urzędu Miasta i Gminy w Chmielniku oraz pracownicy zatrudnieni na stanowiskach samodzielnych, pełniący funkcję redaktorów strony podmiotowej Biuletynu Informacji Publicznej.
2. Do zdań administratora strony podmiotowej BIP należą w szczególności:
a) nadzór nad prawidłowym funkcjonowaniem BIP;
b) określanie sposobu publikowania informacji w BIP oraz przekazywanie wiedzy na ten temat wszystkim członkom zespołu redakcyjnego;
c) publikowanie i aktualizowanie informacji w BIP na wniosek redaktorów strony podmiotowej,
d) rzetelne zamieszczanie w BIP informacji publicznych przeznaczonych do publikacji wraz z oznaczeniem dla każdej z nich: daty wytworzenia, tożsamości osoby która wytworzyła lub odpowiada za treść;
e) udzielanie wszystkim zainteresowanym pomocy i wyjaśnień w zakresie związanym z prowadzeniem BIP;
f) nadzór i podejmowanie niezbędnych czynności w celu zachowania spójności informacji zamieszczanych w BIP;
g) współpraca z dostawcą strony podmiotowej, w tym niezwłoczne zgłaszanie mu informacji o awariach i nieprawidłowościach w technicznym funkcjonowaniu BIP oraz nadzorowanie prawidłowego ich usunięcia.
3. Do zdań zespołu redakcyjnego strony podmiotowej BIP należą w szczególności:
a) współpraca z innymi pracownikami komórki organizacyjnej w zakresie związanym z publikowaniem w BIP informacji, za których wytworzenie lub przechowywanie są oni odpowiedzialni (administratorzy odpowiedzialni są za publikację w BIP, zespół redakcyjny za przygotowanie informacji do publikacji w BIP i przekazanie jej do administratorów za pomocą służbowej skrzynki e-mailowej),
b) nadzór nad zachowaniem zgodności publikowanych w BIP informacji z aktualnym stanem faktycznym i prawnym oraz zachowaniem ich kompletności i spójności;

c) zgłaszaniem administratorowi problemów i nieprawidłowości w funkcjonowaniu strony podmiotowej BIP lub panelu administracyjnego BIP.

§ 3. Kierownik wydziału Urzędu lub pracownik zatrudniony na samodzielnym stanowisku odpowiada za:
1) sprawowanie formalnego i merytorycznego nadzoru nad zakresem i sposobem publikowania w BIP informacji posiadanych lub wytwarzanych przez komórkę organizacyjną, której pracą kieruje;
2) przechowywanie i przetwarzania udostępnionych informacji w BIP zgodnie z obowiązującymi w tym zakresie przepisami prawa między innymi: ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

§ 4. 1.Pracownik, który w ramach swoich kompetencji wytwarza informację publiczną podlegającą publikacji w BIP zobowiązany jest do przekazania administratorowi BIP do publikacji, za pomocą służbowej skrzynki poczty elektronicznej lub wewnętrznej sieci w Urzędzie, a także odpowiada za jej przechowywanie i przetwarzanie na swoim stanowisku pracy/komórce organizacyjnej w której została wytworzona i BIP zgodnie z przepisami prawa, o których mowa w § 3 pkt 2).
2. Publikacja informacji, którą w ramach swoich kompetencji wytworzył lub przechowuje redaktor, następuje na podstawie:
1) informacji przekazanej do administratora za pomocą służbowej skrzynki poczty elektronicznej,
2) informacji przekazanej telefonicznie do administratora o umieszczeniu w folderze Publicznym, informacji do publikacji w BIP (wskazanie nazwy pliku, folderu itp.).

§ 5. 1.Publikowanie informacji w BIP odbywa się zgodnie z wymogami określonymi w ustawie o dostępie do informacji publicznej
2. Informacje publiczne zamieszczane na stronie BIP nie mogą zawierać reklam.
3. O ile przepisy prawa nie określają szczegółowych terminów publikacji, publikacja lub aktualizacja informacji publicznej podlegającej publikacji w BIP powinna zostać wykonana niezwłocznie, nie później jednak niż 60 dni od dnia przekazania informacji do publikacji.
4. Prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, a także ze względu na prywatność osoby fizycznej na podstawie 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) (Dz.U.UE.L.2016.119.1 z dnia 2016.05.04) lub tajemnicę przedsiębiorcy.
5.W przypadku wyłączenia jawności informacji publicznej lub anonimizacji danych osobowych, w BIP umieszcza się komentarz, w którym podaje się zakres wyłączenia, podstawę prawną wyłączenia jawności.
6. W przypadku publikacji kopii dokumentów, wyłączenie jawności ich fragmentów lub anonimizacji danych osobowych, dokonuje się poprzez zakrycie chronionych danych.

7. Wyłączenia jawności lub anonimizacji danych osobowych w informacji publicznej wraz z komentarzem, dokonuje pracownik merytorycznie odpowiedzialny za wytworzenie lub przechowywanie tej informacji.
8. Informacja publiczna może zostać zamieszczona na stronie BIP w postaci plików z danymi w następujących formatach: doc, docx, rtf, pdf, txt, xml, xls, jpg, ppt,zipx. Nazwy plików nie powinny zawierać polskich znaków diakrytycznych. Maksymalny rozmiar pojedynczego pliku: 128 MB.
9. Transmisja i nagranie obrad Rady Miejskiej w Chmielniku udostępniane są w BIP (a także na stronie internetowej Urzędu) za pośrednictwem odnośnika do Kanału Rady Miejskiej w Chmielniku na YouTube: https://www.youtube.com/channel/UCvXePsNgV_Vjt--1JdSubtQ:
a) „Warunki przetwarzania danych osobowych przez YouTube" z dnia 25 maja 2018 r. stanowią załącznik zarządzenia;
b) administrator BIP wykonuje kopie nagrania z danej sesji, archiwizuje plik z nagraniem na serwerze w Urzędzie Miasta i Gminy w Chmielniku i na nośniku np. płyta DVD z odpowiednim opisem;
c) udostępnione nagrania z sesji będę przechowywane przez okres 5 lat od daty publikacji. Po tym czasie dany plik z nagraniem zostanie usunięty. Archiwizacja nagrań będzie obywała się zgodnie z zapisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.
10. Informacja publiczna, która nie została udostępniona w BIP jest udostępniona na wniosek, (wzór wniosku został zamieszczony na w BIP).

§ 6. 1.Uprawnienia do panelu administracyjnego BIP posiadają wyłącznie administratorzy.
2. Nadawanie, modyfikowanie i wycofywanie uprawnień do panelu administracyjnego BIP, odbywa się za pisemną zgodą Burmistrza.

§ 7. Zarządzenie wchodzi w życie z dniem wydania.

BURMISTRZ
Paweł Wójcik

RADCA PRAWNY
Wojciech Chłopek
KL-K-719

załącznik do zarządzenia
Nr 139/2019 z dn. 15.11.2019 r.

Warunki przetwarzania danych osobowych przez YouTube

Data ostatniej aktualizacji: 25 maja 2018 r.

Niniejsze Warunki przetwarzania danych osobowych obowiązujące w YouTube (wraz z załącznikami zwane dalej „**Warunkami przetwarzania danych osobowych**") stosuje się do przetwarzania danych osobowych klienta. Warunki te stanowią dodatek do umowy zawartej pomiędzy klientem („**klient**") a Google, określającej zasady korzystania przez klienta z serwisu YouTube („**Umowa**"). Umowa może zawierać Warunki korzystania z serwisu YouTube lub umowę licencji na korzystanie z treści, odpowiednio do klienta. Prosimy o uważne zapoznanie się z treścią niniejszych Warunków przetwarzania danych osobowych.

1. Wprowadzenie

Niniejsze Warunki przetwarzania danych osobowych dokumentują porozumienie stron w sprawie warunków regulujących przetwarzanie i bezpieczeństwo danych osobowych klienta w kontekście przepisów o ochronie danych osobowych.

2. Definicje i interpretacja

2.1 Poniższe terminy użyte w niniejszych Warunkach przetwarzania danych osobowych mają następujące znaczenie:
„**podmiot powiązany,**" o ile nie został już definiowany w Umowie, oznacza podmiot, który bezpośrednio lub pośrednio kontroluje lub jest kontrolowany przez stronę, lub pozostaje pod wspólną kontrolą ze stroną;
„**dane osobowe klienta**" oznaczają treści audio i audiowizualne przesłane przez klienta do serwisu YouTube zgodnie z postanowieniami Umowy oraz przetwarzane przez Google w imieniu klienta w ramach świadczenia przez Google usług podmiotu przetwarzającego;
„**incydent naruszenia bezpieczeństwa danych osobowych**" oznacza naruszenie bezpieczeństwa Google prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych klienta w systemach informatycznych zarządzanych lub kontrolowanych w inny sposób przez Google. Do „incydentów naruszenia bezpieczeństwa danych osobowych" nie zalicza się nieudanych prób lub działań, które nie naruszają bezpieczeństwa danych osobowych klienta, w tym nieudanych prób zalogowania się, upływu limitu czasu żądania (test ping), skanów portów, ataku typu odmowa usługi oraz innych ataków sieciowych na zapory ogniowe lub systemy działające w sieci;
„**przepisy o ochronie danych osobowych**" oznaczają, stosownie do przypadku: (a) RODO; lub (b) federalną ustawę o ochronie danych osobowych z 19 czerwca 1992 r. (Szwajcaria);
„**narzędzie osoby, której dane dotyczą**" oznacza narzędzie (gdy ma to zastosowanie) udostępnione przez Google osobom, których dane dotyczą, umożliwiające Google reagowanie w sposób bezpośredni i ujednolicony na określone żądania osób, których dane dotyczą, dotyczące danych osobowych klienta (na przykład ustawień w zakresie reklam w Internecie lub wtyczki do przeglądarek umożliwiającej rezygnację z określonych usług);
„**EOG**" oznacza Europejski Obszar Gospodarczy;
„**RODO**" oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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;
„**Google**" oznacza podmiot Google będący stroną Umowy zawartej z klientem;
„**podwykonawcy przetwarzania będący podmiotami powiązanymi Google**" mają znaczenie określone w Punkcie 11.1 (Zgoda na korzystanie z usług podwykonawców przetwarzania);
„**podmiot Google**" oznacza Google LLC (danej Google Inc.), Google Ireland Limited, YouTube, LLC lub dowolny inny podmiot powiązany Google LLC;
„**certyfikat ISO 27001**" oznacza zaświadczenie przyznania certyfikatu ISO/IEC 27001:2013 lub certyfikatu porównywalnego dla usług podmiotu przetwarzającego;
„**adres mailowy do powiadomień**" oznacza adres mailowy (o ile istnieje) wyznaczony przez klienta, za pośrednictwem interfejsu
użytkownika usług podmiotu przetwarzającego lub w inny sposób udostępniony przez Google, do otrzymywania określonych powiadomień od Google dotyczących niniejszych Warunków przetwarzania danych osobowych;
„**Tarcza Prywatności**" oznacza ramy prawne przewidziane przez porozumienie Tarcza Prywatności UE-USA oraz ramy prawne przewidziane przez porozumienie Tarcza Prywatności Szwajcaria-USA;
„**usługi podmiotu przetwarzającego**" oznaczają przetwarzanie danych osobowych klienta zgodnie z niniejszymi Warunkami przetwarzania danych osobowych;
„**dokument bezpieczeństwa**" oznacza zaświadczenie przyznania certyfikatu ISO 27001, o ile istnieje, oraz wszystkie, inne zaświadczenia, certyfikaty lub dokumentacje, które mogą zostać udostępnione przez Google odnośnie usług podmiotu przetwarzającego;
„**środki bezpieczeństwa**" mają znaczenia nadane w Punkcie 7.1.1 (Środki bezpieczeństwa Google);
„**podwykonawcy przetwarzania**" oznaczają strony trzecie uprawnione na podstawie niniejszych Warunków przetwarzania danych osobowych do posiadania logicznego dostępu do i przetwarzania danych osobowych klienta w celu świadczenia części usług podmiotu przetwarzającego oraz wszelkiego, związanego z nimi wsparcia technicznego;
„**podwykonawcy przetwarzania będący stronami trzecimi**" mają znaczenia nadane w Punkcie 11.1 (Zgoda na korzystanie z usług podwykonawców przetwarzania).

2.2 Terminy „**administrator danych**", „**osoba, której dane dotyczą**", „**dane osobowe**", „**przetwarzanie**", „**podmiot**

przetwarzający" i **„organ nadzorczy"** użyte w niniejszych Warunkach przetwarzania danych osobowych mają znaczenie podane w RODO.

2.3 Wszelkie odwołania do ram prawnych, ustawy lub innych aktów prawnych są odwołaniami do tych samych w brzmieniu uwzględniającym wszelkie ich późniejsze zmiany lub nowe wersje.

3. Okres obowiązywania niniejszych Warunków przetwarzania danych osobowych
Okres obowiązywania (**„Okres obowiązywania"**) niniejszych Warunków przetwarzania danych osobowych oraz świadczenia przez Google usług podmiotu przetwarzającego rozpoczyna się 25 maja 2018 r. (lub w dniu podpisania Umowy, jeżeli nastąpi to po 25 maja 2018 r.) (**„Dzień wejścia w życie okresu obowiązywania"**), i trwa do momentu usunięcia wszelkich danych osobowych klienta przez Google w sposób opisany w niniejszych Warunkach przetwarzania danych osobowych.

4. Stosowanie niniejszych Warunków przetwarzania danych osobowych
Stosowanie przepisów o ochronie danych osobowych. Niniejsze Warunki przetwarzania danych osobowych stosuje się jedynie w zakresie, w jakim przepisy o ochronie danych osobowych mają zastosowanie do przetwarzania danych osobowych klienta, w tym w szczególności w przypadku gdy:

(a) przetwarzanie odbywa się w ramach działalności jednostki organizacyjnej klienta mającej siedzibę na terytorium EOG; lub

(b) dane osobowe klienta są danymi osobowymi osób, których dane dotyczą, znajdujących się na terytorium EOG, a przetwarzanie dotyczy oferowania takim osobom towarów lub usług, lub monitorowania ich zachowania na terytorium EOG.

5. Przetwarzanie danych
5.1 **Role i zgodność z przepisami; Zatwierdzenie.**

5.1.1 Zakres obowiązków podmiotu przetwarzającego i administratora danych.

(a) Niniejsze Warunki przetwarzania danych osobowych opisują przedmiot i szczegóły przetwarzania danych osobowych klienta;

(b) Google jest podmiotem przetwarzającym dane osobowe klienta w rozumieniu przepisów o ochronie danych osobowych;

(c) klient jest administratorem danych lub podmiotem przetwarzającym, stosownie do przypadku, danych osobowych klienta w rozumieniu przepisów o ochronie danych osobowych; oraz

(d) każda ze stron jest zobowiązania wypełniać obowiązki spoczywające na niej w rozumieniu przepisów o ochronie danych osobowych w odniesieniu do przetwarzania danych osobowych klienta.

5.1.2 Zatwierdzenie przez administratora danych będącego stroną trzecią. Jeżeli klient jest podmiotem przetwarzającym, klient zapewnia Google, że instrukcje i czynności klienta dotyczące danych osobowych klienta, w tym powołanie przez klienta Google na inny podmiot przetwarzający, zostały zatwierdzone przez właściwego administratora danych.

5.2 **Instrukcje klienta.** Klient nakazuje Google przetwarzanie danych osobowych klienta jedynie zgodnie z właściwym prawem i niniejszymi Warunkami przetwarzania danych osobowych: (a) w celu świadczenia usług podmiotu przetwarzającego oraz związanego z nimi wsparcia technicznego; (b) w sposób wynikający ze sposobu korzystania przez klienta z usług podmiotu przetwarzającego (w tym między innymi w sposób wskazany w ustawieniach lub innych funkcjach usług podmiotu przetwarzającego) oraz związanego z nimi wsparcia technicznego; oraz (c) w sposób udokumentowany we wzorze Umowy, w tym w niniejszych Warunkach przetwarzania danych osobowych.

5.3 **Stosowanie się przez Google do instrukcji.** Google jest zobowiązana stosować się do instrukcji opisanych w Punkcie 5.2 (Instrukcje klienta) (w tym dotyczących przekazywań danych), chyba że prawo UE lub państwa członkowskiego UE, któremu Google podlega, wymaga od Google przetwarzania danych osobowych klienta w inny sposób, w którym to przypadku Google jest zobowiązana poinformować o tym klienta (chyba że prawo zabrania Google informowania o tym klienta z uwagi na ważne względy interesu publicznego).

6. Usuwanie danych
6.1 **Usuwanie danych w trakcie Okresu obowiązywania.**

6.1.1 Usługi podmiotu przetwarzającego wyposażone w funkcję usuwania danych. Jeżeli w trakcie Okresu obowiązywania:

(a) wśród funkcji oferowanych w ramach usług podmiotu przetwarzającego jest oferowana opcja umożliwiająca klientowi usunięcie danych osobowych klienta;

(b) klient korzysta z usług podmiotu przetwarzającego w celu usunięcia określonych danych osobowych klienta; oraz

(c) usunięte dane osobowe klienta nie mogą zostać odzyskane przez klienta (na przykład z foldera „śmieci"),

wówczas Google usuwa takie dane osobowe klienta ze swoich systemów informatycznych tak szybko, jak to jest praktycznie możliwe, chyba że prawo UE lub państwa członkowskiego UE wymaga, aby dane takie były przechowywane.

6.1.2 Usługi podmiotu przetwarzającego bez funkcji usuwania danych. Jeżeli w trakcie Okresu obowiązywania wśród funkcji oferowanych w ramach usług podmiotu przetwarzającego nie jest oferowana opcja umożliwiająca klientowi usunięcie danych osobowych klienta, wówczas Google na uzasadnione żądanie klienta umożliwia takie usunięcie pod warunkiem, że jest to możliwe, uwzględniając charakter i funkcje oferowane w ramach usług podmiotu przetwarzającego. Google może pobierać opłatę (obliczoną w oparciu o zasadnie poniesione koszty Google) za usunięcie danych zgodnie z niniejszym Punktem 6.1.2 (Usługi podmiotu przetwarzającego bez funkcji usuwania danych). Google przekazuje klientowi szczegółowe informacje na temat odpowiedniej opłaty oraz podstawy jej wyliczenia, przed usunięciem takich danych.

6.2 **Usunięcie danych po wygaśnięciu Umowy.** Po wygaśnięciu, rozwiązaniu lub wypowiedzeniu Umowy klient nakazuje Google usunięcie wszelkich danych osobowych klienta (w tym dotychczasowych kopii) z systemów informatycznych Google zgodnie z właściwym prawem. Google zobowiązana jest zastosować się to takiej instrukcji tak szybko, jak to jest praktycznie możliwe, chyba że: (i) prawo UE lub państwa członkowskiego UE wymaga, aby dane takie były przechowywane; lub (ii) Umowa zostanie zastąpiona przez nową umowę lub warunki pomiędzy klientem a Google dotyczące korzystania przez klienta z serwisu YouTube i klient potwierdzi, że dane osobowe klienta (w tym dotychczasowe ich kopie już przesłane do serwisu YouTube) powinny być nadal przetwarzane zgodnie z niniejszymi Warunkami przetwarzania danych osobowych.

7. Bezpieczeństwo danych
7.1 **Środki bezpieczeństwa i pomoc Google.**

7.1.1 Środki bezpieczeństwa Google. Google wdraża i utrzymuje w sprawności techniczne i organizacyjne środki ochrony danych osobowych klienta przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, nieuprawnionym ujawnieniem lub dostępem, w sposób opisany z Załączniku 2 (**„Środki bezpieczeństwa"**). Google może aktualizować lub modyfikować środki bezpieczeństwa w dowolnym momencie pod warunkiem, że takie aktualizacje i modyfikacje nie spowodują pogorszenia ogólnego bezpieczeństwa usług podmiotu przetwarzającego.

7.1.2 Przestrzeganie zasad bezpieczeństwa danych osobowych przez pracowników Google. Google jest zobowiązana zapewnić, aby wszystkie osoby

uprawnione do przetwarzania danych osobowych klienta zobowiązały się do zachowania poufności lub podlegały stosownemu ustawowemu obowiązkowi zachowania poufności.

7.1.3 Pomoc Google w ochronie bezpieczeństwa danych osobowych. Google jest zobowiązana (ze względu na charakter przetwarzania danych osobowych klienta oraz informacje dostępne dla Google) pomagać klientowi w zapewnianiu wypełniania wszelkich obowiązków klienta w zakresie bezpieczeństwa danych osobowych i naruszeń danych osobowych, w tym (gdy ma to zastosowanie) obowiązków klienta wynikających z art. 32-34 RODO, poprzez:

(a) wdrożenie i utrzymywanie w sprawności środków bezpieczeństwa zgodnie z Punktem 7.1.1 (Środki bezpieczeństwa Google);

(b) stosowanie się do postanowień Punktu 7.2 (Incydenty naruszenia bezpieczeństwa danych osobowych); oraz

(c) dostarczenie klientowi dokumentu bezpieczeństwa zgodnie z Punktem 7.5.1 (Wgląd do dokumentu bezpieczeństwa) i informacji zawartych w niniejszych Warunkach przetwarzania danych osobowych.

7.2 **Incydenty naruszenia bezpieczeństwa danych osobowych.**

7.2.1 Powiadamianie o incydentach naruszenia bezpieczeństwa danych osobowych. Jeżeli Google poweźmie wiadomość o incydencie naruszenia bezpieczeństwa danych osobowych, Google: (a) powiadomi klienta o incydencie naruszenia bezpieczeństwa danych osobowych niezwłocznie i bez zbędnej zwłoki; oraz (b) niezwłocznie podejmie racjonalnie uzasadnione kroki w celu minimalizacji szkody i zabezpieczenia danych osobowych klienta.

7.2.2 Szczegóły incydentu naruszenia bezpieczeństwa danych osobowych. Powiadomienia dokonywane zgodnie z Punktem 7.2.1 (Powiadamianie o incydentach naruszenia bezpieczeństwa danych osobowych) winny opisywać, w miarę możliwości, szczegóły incydentu naruszenia bezpieczeństwa danych osobowych, w tym kroki podjęte w celu minimalizacji potencjalnego ryzyka oraz kroki, których podjęcie Google rekomenduje klientowi w celu zaradzenia incydentowi naruszenia bezpieczeństwa danych osobowych.

7.2.3 Dostarczenie powiadomienia. Google dostarcza powiadomienia o incydencie naruszenia bezpieczeństwa danych osobowych na adres mailowy do powiadomień lub za pośrednictwem innych środków komunikacji bezpośredniej (na przykład telefonicznie lub podczas spotkania osobistego). Klient podejmie wszelkie racjonalnie uzasadnione kroki w celu dostarczenia adresu mailowego do powiadomień i zapewnienia, aby adres mailowy do powiadomień był aktualny i aktywny.

7.2.4 Powiadamianie stron trzecich o incydentach naruszenia bezpieczeństwa danych osobowych. Klient ponosi wyłączną odpowiedzialność za stosowanie się do przepisów dotyczących powiadamiania o incydentach naruszenia bezpieczeństwa danych osobowych mających zastosowanie do klienta oraz za wypełnianie obowiązków powiadamiania stron trzecich o incydentach naruszenia bezpieczeństwa danych osobowych.

7.2.5 Brak uznania winy przez Google. Powiadomienie o incydencie naruszenia bezpieczeństwa danych osobowych lub reakcja na taki incydent przez Google zgodnie z niniejszym Punktem 7.2 (Incydenty naruszenia bezpieczeństwa danych osobowych) nie może być interpretowane jako uznanie przez Google winy lub odpowiedzialności za incydent naruszenia bezpieczeństwa danych osobowych.

7.3 **Zakres odpowiedzialności klienta za bezpieczeństwo oraz ocena bezpieczeństwa przez klienta.**

7.3.1 Zakres odpowiedzialności klienta za bezpieczeństwo. Nie naruszając obowiązków Google przewidzianych w Punktach 7.1 (Środki bezpieczeństwa i pomoc Google) i 7.2 (Incydenty naruszenia bezpieczeństwa danych osobowych):

(a) klient ponosi wyłączną odpowiedzialność za korzystanie z usług podmiotu przetwarzającego, w tym między innymi za:

(i) właściwe korzystanie z usług podmiotu przetwarzającego w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka, na jakie narażone są dane osobowe klienta; oraz

(ii) zabezpieczenie danych wykorzystywanych do autoryzacji konta, systemów informatycznych i urządzeń wykorzystywanych przez klienta do dostępu do usług podmiotu przetwarzającego; oraz

(b) Google nie ma obowiązku chronienia danych osobowych klienta, które klient postanowił przechowywać lub przesłać poza systemami informatycznymi Google oraz podwykonawców przetwarzania Google.

7.3.2 Ocena bezpieczeństwa przez klienta. Klient przyjmuje do wiadomości i akceptuje, że (ze względu na stan wiedzy technicznej, koszty wdrożenia a także charakter, zakres, kontekst i cele przetwarzania danych osobowych klienta i ryzyka, na jakie narażone są osoby fizyczne) środki bezpieczeństwa wdrożone i utrzymywane w sprawności przez Google zgodnie z Punktem 7.1.1 (Środki bezpieczeństwa Google) zapewniają poziom bezpieczeństwa odpowiedni do ryzyka, na jaki narażone są dane osobowe klienta.

7.4 **Certyfikacja bezpieczeństwa.** W celu oceny i ułatwienia zapewnienia stałej skuteczności środków bezpieczeństwa Google może w dowolnym momencie uzyskać certyfikat ISO 27001.

7.5 **Wgląd do dokumentu bezpieczeństwa i kontrole.**

7.5.1 Wgląd do dokumentu bezpieczeństwa. W celu wykazania wypełniania przez Google obowiązków wynikających z niniejszych Warunków przetwarzania danych osobowych Google udostępni klientowi do wglądu dokument bezpieczeństwa.

7.5.2 Prawa klienta do kontroli.

(a) Google zezwoli klientowi lub audytorowi będącemu stroną trzecią wyznaczonemu przez klienta na przeprowadzenie kontroli (w tym również inspekcji) w celu weryfikacji wypełniania przez Google obowiązków wynikających z niniejszych Warunków przetwarzania danych osobowych zgodnie z Punktem 7.5.3 (Dodatkowe warunki przeprowadzania kontroli). Google będzie włączał się w takie kontrole w sposób opisany w Punkcie 7.4 (Certyfikacja bezpieczeństwa) i niniejszym Punkcie 7.5 (Wgląd do dokumentu bezpieczeństwa i kontrole).

(b) Klient może również przeprowadzić kontrolę w celu weryfikacji wypełniania przez Google obowiązków wynikających z niniejszych Warunków przetwarzania danych osobowych poprzez zapoznanie się z zaświadczeniem przyznania certyfikatu ISO 27001 (który odzwierciedla wynik kontroli przeprowadzonej przez kontrolera będącego stroną trzecią), o ile takie zaświadczenie jest dostępne w momencie zgłoszenia przez klienta stosownego żądania.

7.5.3 Dodatkowe warunki przeprowadzania kontroli.

(a) Klient przesyła Google żądanie przeprowadzenia kontroli, o której mowa w Punkcie 7.5.2(a), w sposób opisany w Punkcie 12.1 (Kontakt z Google).

(b) Po otrzymaniu przez Google żądania, o którym mowa w Punkcie 7.5.3(a), Google i klient omawiają i uzgadniają z wyprzedzeniem możliwy termin rozpoczęcia, zakres, czas trwania oraz środki służące zapewnieniu bezpieczeństwa i poufności mające zastosowanie do kontroli, o której mowa w Punkcie 7.5.2(a).

(c) Google może pobierać opłatę (obliczoną w oparciu o zasadnie poniesione koszty Google) za przeprowadzenie kontroli, o której mowa w Punkcie 7.5.2(a). Google przekazuje klientowi szczegółowe informacje na temat odpowiedniej opłaty oraz podstawy jej wyliczenia przed rozpoczęciem każdej takiej kontroli. Klient

ponosi odpowiedzialność za wszelkie opłaty pobierane przez kontrolerów będących stronami trzecimi wyznaczonych przez klienta do przeprowadzenia kontroli.

(d) Google może wyrazić sprzeciw wobec kontrolera będącego stroną trzecią wyznaczonego przez klienta do przeprowadzenia kontroli, o której mowa w Punkcie 7.5.2(a), jeżeli kontroler jest, w uzasadnionej ocenie Google, nieodpowiednio wykwalifikowany lub niewystarczająco niezależny, konkurentem Google lub jest w inny sposób wyraźnie nieodpowiedni. W przypadku zgłoszenia takiego sprzeciwu przez Google klient jest zobowiązany powołać nowego kontrolera lub przeprowadzić kontrolę samodzielnie.

(e) Żadne z postanowień niniejszych Warunkach przetwarzania danych osobowych nie nakłada na Google obowiązku ujawnienia klientowi lub kontrolerowi będącemu stroną trzecią wyznaczonemu przez klienta, ani zezwolenia klientowi lub kontrolerowi będącemu stroną trzecią wyznaczonemu przez klienta na dostęp do:

(i) danych innych klientów dowolnego podmiotu Google;

(ii) wewnętrznych informacji księgowych lub finansowych dowolnego podmiotu Google;

(iii) tajemnic handlowych dowolnego podmiotu Google;

(iv) informacji, które, w uzasadnionej ocenie Google, mogłyby: (A) narazić na szwank bezpieczeństwo systemów informatycznych lub pomieszczeń dowolnego podmiotu Google; lub (B) spowodować naruszenie przez dowolny podmiot Google jego obowiązków wynikających z przepisów o ochronie danych osobowych lub jego obowiązków w zakresie bezpieczeństwa i ochrony poufności wobec klienta lub dowolnej strony trzeciej; lub

(v) informacji, do których klient lub wyznaczony przez niego kontroler będący stroną trzecią stara się uzyskać dostęp z powodów innych niż wypełnianie w dobrej wierze obowiązków klienta wynikających z przepisów o ochronie danych osobowych.

8. Ocena skutków dla ochrony danych i konsultacje
Google (ze względu na charakter przetwarzania danych osobowych klienta oraz informacje dostępne dla Google) pomaga klientowi w zapewnianiu wypełniania wszelkich obowiązków klienta w zakresie oceny skutków dla ochrony danych oraz uprzednich konsultacji, w tym (gdy ma to zastosowanie) obowiązków klienta wynikających z art. 35 i 36 RODO, poprzez:

(a) dostarczanie dokumentu bezpieczeństwa zgodnie z Punktem 7.5.1 (Przeglądy dokumentu bezpieczeństwa);

(b) dostarczanie informacji zawartych w niniejszych Warunkach przetwarzania danych osobowych; oraz

(c) dostarczanie lub udostępnianie w inny sposób, zgodnie ze standardowymi praktykami Google, innych materiałów dotyczących charakteru usług podmiotu przetwarzającego i przetwarzania danych osobowych klienta (na przykład materiałów na temat funkcjonowania centrum pomocy).

9. Prawa osób, których dane dotyczą
9.1 **Odpowiadanie na żądania osób, których dane dotyczą.** Jeżeli Google otrzyma żądanie od osoby, której dane dotyczą, dotyczące danych osobowych klienta, Google:

(a) jeżeli żądanie zostało przesłane przy pomocy narzędzia osoby, której dane dotyczą, odpowiada bezpośrednio na żądanie osoby, której dane dotyczą, w sposób przewidziany w funkcji takiego narzędzia osoby, której dane dotyczą; lub

(b) jeżeli żądanie nie zostało przesłane przy pomocy narzędzia osoby, której dane dotyczą, informuje osobę, której dane dotyczą, aby przesłała swoje żądanie do klienta, i to klient ponosi odpowiedzialność za odpowiedź na takie żądanie.

9.2 **Pomoc Google w odpowiadaniu na żądania osób, których dane dotyczą.** Google (ze względu na charakter przetwarzania danych osobowych klienta oraz, w stosownych przypadkach, postanowienia art. 11 RODO) pomaga klientowi w wypełnianiu przez klienta jego obowiązku odpowiadania na żądania osób, których dane dotyczą, w tym między innymi (gdy ma to zastosowanie) obowiązku odpowiadania przez klienta na żądania osób, których dane dotyczą, o możliwość skorzystania z praw określonych w Rozdziale III RODO, poprzez:

(a) zapewnienie odpowiedniej funkcji w ramach usług podmiotu przetwarzającego;

(b) wypełnianie obowiązków, o których mowa w Punkcie 9.1 (Odpowiadanie na żądania osób, których dane dotyczą); oraz

(c) o ile ma zastosowanie do usług podmiotu przetwarzającego, udostępnianie narzędzi osoby, której dane dotyczą.

10. Przekazywania danych
10.1 **Obiekty wykorzystywane do przechowywania i przetwarzania danych.** Google może, z zastrzeżeniem Punktu 10.2 (Przekazywania danych poza terytorium EOG i Szwajcarii), przechowywać i przetwarzać dane osobowe klienta na terytorium Stanów Zjednoczonych oraz dowolnego, innego kraju, w którym Google lub jej podwykonawcy przetwarzania posiadają swoje obiekty.

10.2 **Przekazywania danych poza terytorium EOG i Szwajcarii.** Google zapewnia, że:

(a) spółka dominująca Grupy Google, Google LLC, będzie nadal deklarować przestrzeganie zasad Tarczy Prywatności w swoim w własnym imieniu oraz w imieniu swoich całkowicie zależnych spółek ze Stanów Zjednoczonych; oraz

(b) zakres deklaracji przez Google LLC przestrzegania zasad Tarczy Prywatności będzie obejmował dane osobowe klienta.

10.3 **Informacje o centrach danych.** Informacje o lokalizacjach centrów danych Google dostępne są na stronie: www.google.com/about/datacenters/inside/locations/index.html.

11. Podwykonawcy przetwarzania
11.1 **Zgoda na korzystanie z usług podwykonawców przetwarzania.** Klient w sposób wyraźny wyraża zgodę na korzystanie z usług podmiotów powiązanych Google jako podwykonawców przetwarzania („**podwykonawcy przetwarzania będący podmiotami powiązanymi Google**"). Dodatkowo klient co do zasady wyraża zgodę na korzystanie z usług dowolnych innych stron trzecich jako podwykonawców przetwarzania („**podwykonawcy przetwarzania będący stronami trzecimi**").

11.2 **Informacje o podwykonawcach przetwarzania.** Informacje o podwykonawcach przetwarzania dostępne są na stronie privacy.google.com/businesses/subprocessors.

11.3 **Wymagania w zakresie korzystania z usług podwykonawców przetwarzania.** W momencie korzystania z usług dowolnego podwykonawcy przetwarzania Google:

(a) zapewnia w drodze pisemnej umowy, że:

(i) podwykonawca przetwarzania ma dostęp do i wykorzystuje dane osobowe klienta jedynie w zakresie wymaganym do wypełniania powierzonych mu obowiązków oraz zgodnie z Umową (w tym niniejszymi Warunkami przetwarzania danych osobowych) i Tarczą Prywatności; oraz

(ii) jeżeli postanowienia RODO mają zastosowanie do przetwarzania danych osobowych klienta, obowiązki dotyczące ochrony danych przewidziane w art. 28(3)

Redundantność. Systemy infrastrukturalne zostały zaprojektowane w celu wyeliminowania pojedynczych punktów podatności na awarie oraz zminimalizowania wpływu potencjalnych ryzyk, na jakie narażone jest środowisko informatyczne. Redundatność uzyskuje się, dublując obwody, przełączniki, sieci lub inne, niezbędne urządzenia. Usługi podmiotu przetwarzającego zostały zaprojektowane w sposób umożliwiający Google wykonywanie określonych rodzajów czynności konserwacji naprawczej i prewencyjnej bez przerw w działaniu. Dla wszystkich urządzeń i obiektów wchodzących w skład środowiska informatycznego zostały opracowane i udokumentowane procedury wykonywania czynności konserwacji prewencyjnej, opisujące w sposób szczegółowy procedurę i częstotliwość wykonywania takich czynności zgodnie ze specyfikacją producenta lub wewnętrzną. Czynności konserwacji prewencyjnej i naprawczej wykonywane w odniesieniu do sprzętu centrów danych są planowane w ramach standardowego procesu, zgodnie z udokumentowanymi procedurami.

Zasilanie. Instalacje zasilające centra danych w energię elektryczną zostały zaprojektowane w sposób zapewniający ich redundantność oraz umożliwiający ich konserwację i naprawę bez wpływu na ciągłość działania całodobowo, siedem dni w tygodniu. W większości przypadków krytyczne komponenty infrastruktury centrów danych zasilane są zarówno przez główne, jak i alternatywne źródło energii elektrycznej posiadające taką samą moc. Zapasowe zasilanie energią elektryczną zapewniają różne mechanizmy, takie jak akumulatory zasilaczy awaryjnych (UPS), które zapewniają niezawodną i stałą gwarancję dostawy energii elektrycznej w trakcie częściowej lub całkowitej przerwy w dostawie energii elektrycznej, przepięcia, podnapięcia i wahań częstotliwości niemieszczących się w granicach tolerancji. W przypadku przerwy w dostawie energii elektrycznej uruchamia się zapasowe źródło zasilania, które dostarcza energię elektryczną do centrum danych w okresie przejściowym, z pełną mocą, przez okres maksymalnie 10 minut, dopóki nie zostaną uruchomione i nie zaczną dostarczać energii elektrycznej instalacje agregatów prądotwórczych wysokoprężnych. Agregaty prądotwórcze wysokoprężne są w stanie uruchomić się automatycznie w ciągu kilku sekund i dostarczać podczas awarii ilość energii elektrycznej wystarczającą do pracy centrum danych z pełną mocą przez okres wielu dni.

Systemy operacyjne serwerów. Serwery Google korzystają z systemów operacyjnych o zwiększonym poziomie bezpieczeństwa, indywidualnie dostosowanych do unikalnych wymagań stawianych przed serwerami w naszej branży. Do przechowywania danych wykorzystujemy nasze autorskie algorytmy, aby poprawić bezpieczeństwo danych i zwiększyć redundantność. Google stosuje proces przeglądów kodów w celu poprawy bezpieczeństwa kodu wykorzystywanego do świadczenia usług podmiotu przetwarzającego i udoskonalenia produktów bezpieczeństwa w środowisku produkcyjnym.

Ciągłość działalności. Google replikuje dane w wielu systemach, aby móc lepiej chronić dane przed ich przypadkowym zniszczeniem lub utratą. Google opracowała i regularnie planuje i testuje programy planowania ciągłości działalności oraz plany odzysku danych i poawaryjnego przywracania systemów.

(b) Sieci i przesyłanie.

Przesyłanie danych. Centra danych są zazwyczaj połączone szybkimi łączami prywatnymi w celu zapewnienia bezpiecznego i szybkiego przesyłu danych między centrami danych. Takie rozwiązanie ma na celu niedopuszczenie do nieuprawnionego odczytu, skopiowania, zmiany lub usunięcia danych w trakcie przesyłu lub transportu elektronicznego, lub podczas zapisu na nośnikach danych. Google przesyła dane, korzystając ze standardowych protokołów internetowych.

Ochrona przed atakami z zewnątrz. Google chroni swoją zewnętrzną powierzchnię ataku przy pomocy wielowarstwowych poziomów zabezpieczeń urządzeń sieciowych oraz systemów wykrywania wtargnięć. Google analizuje potencjalne wektory ataku i wbudowuje odpowiednie, specjalnie opracowane technologie w zewnętrzne systemy informatyczne.

Wykrywanie wtargnięć. Wykrywanie wtargnięć służy uzyskaniu wiedzy na temat potencjalnych ataków oraz odpowiednich informacji koniecznych do reagowania na incydenty. System wykrywania wtargnięć stosowany przez Google obejmuje:

1. ścisłą kontrolę wielkości i składu powierzchni ataku Google poprzez stosowanie środków i czynności zaradczych;

2. stosowanie inteligentnych mechanizmów wykrywania w punktach wprowadzania danych; oraz

3. stosowanie technologii automatycznie naprawiających niektóre sytuacje niebezpieczne.

Reagowanie na incydenty. Google monitoruje różne kanały komunikacji w celu wykrywania incydentów dotyczących bezpieczeństwa, a personel Google odpowiedzialny za bezpieczeństwo reaguje niezwłocznie na znane incydenty.

Technologie szyfrowania. Google udostępnia szyfrowanie HTTPS (zwane również SSL lub łącze TLS). Serwery Google wykorzystują protokół uzgadniania kluczy krzywej eliptycznej Diffiego-Hellmana, przy użyciu kluczy RSA i ECDSA. Te metody perfekcyjnego utajnienia przekazywania (PFS) pomagają chronić ruch danych i minimalizować ujemny wpływ odtajnienia kluczy lub złamania szyfru.

2. **Mechanizmy kontroli dostępu i obiektów**

(a) Mechanizmy kontroli obiektów.

Ochrona fizyczna centrów danych. W centrach danych Google działają wewnętrzne działy zapewnienia bezpieczeństwa odpowiedzialne za fizyczną ochronę wszystkich funkcji centrów danych przez całą dobę, siedem dni w tygodniu. Personel wewnętrznego działu zapewnienia bezpieczeństwa monitoruje obiekty przy pomocy instalacji telewizyjnego systemu nadzoru oraz systemów alarmowych. Personel wewnętrznego działu zapewnienia bezpieczeństwa regularnie patroluje teren wokół oraz wewnątrz centrów danych.

Procedura dostępu do centrów danych. Google stosuje formalne procedury kontroli fizycznego dostępu do centrów danych. Centra danych znajdują się w obiektach, do których można wejść tylko przy użyciu karty z elektronicznym kluczem dostępowym, wyposażonych w alarmy połączone z wewnętrznym działem zapewnienia bezpieczeństwa. Wszyscy wchodzący do centrum danych muszą się przedstawić oraz wylegitymować personelowi wewnętrznego działu zapewnienia bezpieczeństwa. Do centrów danych mogą wejść tylko uprawnieni pracownicy, wykonawcy i goście. O wydanie karty z elektronicznym kluczem dostępowym do tych obiektów mogą ubiegać się wyłącznie uprawnieni pracownicy i wykonawcy. Wniosek o wydanie karty z elektronicznym kluczem dostępowym należy złożyć w wyprzedzeniem, pisemnie, a zatwierdzają je przełożony wnioskodawcy oraz dyrektor centrum danych. Wszystkie pozostałe osoby, które muszą uzyskać tymczasowy dostęp do centrum danych, są zobowiązane: (i) uzyskać uprzednią zgodę dyrektora centrum danych na dostęp do konkretnego centrum danych oraz konkretnych obszarów centrum, które chcą odwiedzić; (ii) zarejestrować się w rejestrze gości powadzonym przez wewnętrzny dział zapewnienia bezpieczeństwa; oraz (iii) okazać dokument identyfikujący daną osobę, jako osobę, która uzyskała zgodę na dostęp do centrum danych.

Urządzenia stosowane do fizycznej ochrony centrów danych. W centrach danych Google stosowane są karty z elektronicznym kluczem dostępu oraz biometryczne systemy kontroli dostępu podłączone do systemu alarmowego. System kontroli dostępu monitoruje i rejestruje kartę z elektronicznym kluczem dostępu każdej osoby w momencie gdy wchodzi ona drzwiami głównymi oraz do pomieszczeń wysyłania i odbioru przesyłek i do innych krytycznych pomieszczeń i obszarów. Nieuprawniona aktywność oraz nieudane próby uzyskania dostępu są logowane przez system kontroli dostępu i badane, stosownie do sytuacji. Uprawniony dostęp osób do obszarów biznesowych i centrów danych jest ograniczony w oparciu o wydzielone strefy i zakres obowiązków służbowych osób. Drzwi pożarowe w centrach danych są wyposażone w alarm. Kamery instalacji telewizyjnego systemu nadzoru działają wewnątrz jak i na zewnątrz centrów danych. Kamery są rozmieszczone w taki sposób, aby obejmować swoim zasięgiem obszary strategiczne, w tym między innymi teren okalający, drzwi do budynku centrum danych oraz do pomieszczeń wysyłki i odbioru przesyłek. Personel wewnętrznego działu zapewnienia bezpieczeństwa zarządza sprzętem i urządzeniami instalacji telewizyjnego systemu nadzoru, rejestrowania i kontroli. Bezpieczne okablowanie całego terenu centrum handlowego zapewnia łączność pomiędzy urządzeniami instalacji telewizyjnego systemu nadzoru. Kamery rejestrują obraz terenu obiektu dwadzieścia cztery godziny na dobę, siedem dni w tygodniu. Nagrania są przechowywane przez co najmniej siedem dni, w zależności od aktywności.

(b) Kontrola dostepu.

RODO zostają nałożone na podwykonawcę przetwarzania; oraz

(b) ponosi pełną odpowiedzialność za wszystkie obowiązki powierzone podwykonawcy przetwarzania oraz za wszystkie jego działania i zaniechania.

12. Kontakt z Google; Rejestrowanie czynności przetwarzania
12.1 **Kontakt z Google.** Klient może skontaktować się z Google w sprawie skorzystania z praw przysługujących klientowi na podstawie niniejszych Warunków przetwarzania danych osobowych, korzystając z metod opisanych na stronie http://support.google.com/youtube/?p=data_processing_terms_troubleshooter lub w inny sposób wskazany przez Google w dowolnym momencie.

12.2 **Rejestrowanie czynności przetwarzania przez Google.** Klient przyjmuje do wiadomości, że Google jest zobowiązana na podstawie RODO: (a) zbierać i rejestrować określone informacje, w tym między innymi imię i nazwisko oraz dane kontaktowe każdego podmiotu przetwarzającego lub administratora danych, w imieniu których Google występuje, oraz (gdy ma to zastosowanie) lokalnych przedstawicieli takich podmiotów przetwarzających lub administratorów danych oraz inspektora ochrony danych; oraz (b) udostępniać takie informacje organom nadzorczym. W związku z tym klient, na żądanie oraz gdy ma to zastosowanie do klienta, przekazuje takie informacje Google za pośrednictwem interfejsu użytkownika usług podmiotu przetwarzającego lub w inny sposób zapewniony przez Google, oraz korzysta z takiego interfejsu użytkownika lub innego sposobu w celu zapewnienia, aby wszelkie dostarczone informacje pozostały dokładne i aktualne.

13. Odpowiedzialność
Niezależnie od pozostałych postanowień niniejszej Umowy łączna, sumaryczna odpowiedzialność każdej ze stron wobec drugiej strony wynikająca z lub dotycząca niniejszych Warunków przetwarzania danych osobowych jest ograniczona do maksymalnej kwoty pieniężnej lub kwoty wypłat, do której ograniczona jest odpowiedzialność strony z tytułu Umowy (tytułem wyjaśnienia, wyłączenie roszczeń z tytułu odpowiedzialności za naruszenie poufności lub z tytułu zwolnienia z odpowiedzialności przewidziane postanowieniami Umowy dotyczącymi ograniczenia odpowiedzialności nie mają zastosowania do roszczeń zgłoszonych na podstawie Umowy dotyczących przepisów o ochronie danych osobowych). Żadne z postanowień niniejszego Punktu 13 (Odpowiedzialność) nie wyłącza ani nie ogranicza odpowiedzialności strony za: (a) zgon lub uszkodzenie ciała będące wynikiem niedbalstwa takiej strony lub jej pracowników bądź przedstawicieli; (b) oszustwa lub poświadczenia nieprawdy; lub (c) spraw rodzących odpowiedzialność, której nie można wykluczyć ani ograniczyć na podstawie obowiązującego prawa.

14. Rozstrzygająca moc niniejszych Warunków przetwarzania danych osobowych
W przypadku jakiegokolwiek konfliktu lub rozbieżności pomiędzy treścią niniejszych Warunków przetwarzania danych osobowych a resztą Umowy, niniejsze Warunki przetwarzania danych osobowych będą miały moc rozstrzygającą. Ewentualne zmiany niniejszych Warunków przetwarzania danych osobowych pozostają bez wpływu na ważność i obowiązywanie Umowy.

15. Zmiany niniejszych Warunków przetwarzania danych osobowych
15.1 **Zmiany usług podmiotu przetwarzającego.** Google może zmienić listę potencjalnych usług podmiotu przetwarzającego jedynie w celu:

(a) zmiany nazwy usługi;

(b) dodania nowej usługi; lub

(c) usunięcia usługi w przypadku gdy: (i) wszystkie umowy świadczenia danej usługi zostały rozwiązane lub wypowiedziane; lub (ii) Google uzyskała na to zgodę klienta.

15.2 **Zmiany Warunków przetwarzania danych osobowych.** Google może zmienić niniejsze Warunki przetwarzania danych osobowych, jeżeli zmiana:

(a) jest wyraźnie dozwolona przez niniejsze Warunki przetwarzania danych osobowych, w tym w przypadkach opisanych w Punkcie 15.1;

(b) zmienia firmę lub formę prawną podmiotu prawnego;

(c) jest wymagana w celu przestrzegania mającego zastosowanie prawa lub przepisu, wykonania nakazu sądowego lub zastosowania się do wytycznych wydanych przez organ regulacyjny lub agendę rządową; lub

(d) (i) nie pogarsza ogólnego bezpieczeństwa usług podmiotu przetwarzającego; (ii) nie rozszerza zakresu oraz nie usuwa ograniczeń przetwarzania przez Google danych osobowych klienta, o których mowa w Punkcie 5.3 (Stosowanie się przez Google do instrukcji); oraz (iii) w ocenie Google, nie narusza w inny, istotny sposób praw klienta wynikających z niniejszych Warunków przetwarzania danych osobowych.

Załącznik 1: Przedmiot i szczegóły przetwarzania danych osobowych

Przedmiot

Świadczenie przez Google usług podmiotu przetwarzającego oraz związanego z nimi wsparcia technicznego na rzecz klienta.

Czas trwania przetwarzania

Okres obowiązywania plus okres od momentu upływu Okresu obowiązywania do momentu usunięcia wszelkich danych osobowych klienta przez Google zgodnie z niniejszymi Warunkami przetwarzania danych osobowych.

Charakter i cel przetwarzania

Google przetwarza (w tym między innymi, stosownie do usług podmiotu przetwarzającego i instrukcji opisanych w Punkcie 5.2 (Instrukcje klienta), zbiera, rejestruje, organizuje, porządkuje, przechowuje, zmienia, wyszukuje, wykorzystuje, ujawnia, łączy, usuwa i niszczy) dane osobowe klienta w celu świadczenia usług podmiotu przetwarzającego oraz związanego z nimi wsparcia technicznego na rzecz klienta zgodnie z niniejszymi Warunkami przetwarzania danych osobowych.

Kategorie danych osobowych

Do kategorii danych osobowych stanowiących dane osobowe klienta należą treści audio i audiowizualne przesyłane przez klienta do serwisu YouTube zgodnie z postanowieniami Umowy i przetwarzane przez Google w imieniu klienta w ramach świadczenia przez Google usług podmiotu przetwarzającego.

Załącznik 2: Środki bezpieczeństwa

Począwszy od Dnia wejścia w życie okresu obowiązywania Google wdraża i zapewnia utrzymanie w sprawności środków bezpieczeństwa opisanych w niniejszym Załączniku 2. Google może aktualizować lub modyfikować środki bezpieczeństwa w dowolnym momencie pod warunkiem, że takie aktualizacje i modyfikacje nie spowodują pogorszenia ogólnego bezpieczeństwa usług podmiotu przetwarzającego.

1. **Bezpieczeństwo centrów danych i sieci**

(a) Centra danych.

Infrastruktura. Google posiada rozproszone geograficznie centra danych. Google przechowuje wszystkie dane produkcyjne w fizycznie bezpiecznych centrach danych.

Personel ochrony infrastruktury. Google posiada i stosuje politykę bezpieczeństwa obowiązującą personel ochrony infrastruktury. Zgodnie z tą polityką personel ochrony infrastruktury jest zobowiązany odbywać szkolenie z zakresu bezpieczeństwa w ramach ogólnego szkolenia personelu. Personel ochrony infrastruktury Google jest odpowiedzialny za bieżący monitoring bezpieczeństwa infrastruktury Google, przegląd usług podmiotu przetwarzającego oraz reagowanie na incydenty dotyczące bezpieczeństwa.

Zarządzanie kontrolą dostępu i przywilejami. Administratorzy i użytkownicy klienta muszą uwierzytelnić się za pomocą centralnego systemu uwierzytelniania lub systemu rejestracji wpisów, aby móc skorzystać z usług podmiotu przetwarzającego.

Wewnętrzne procedury i polityki dostępu do danych – Polityka dostępu. Wewnętrzne procedury i polityki dostępu do danych Google mają na celu niedopuszczenie do uzyskania przez nieuprawnione osoby lub systemy dostępu do systemów wykorzystywanych do przetwarzania danych osobowych. Google projektuje swoje systemy w taki sposób: (i) aby tylko osoby uprawnione mogły uzyskać dostęp do danych, do których są one uprawnione mieć dostęp, oraz (ii) aby nie dopuścić do tego, aby dane osobowe mogły być odczytane, skopiowane, zmienione ani usunięte bez autoryzacji w trakcie ich przetwarzania, wykorzystywania i po zapisaniu. Systemy są zaprojektowane, aby wykryć każdy nieuprawniony dostęp. Google stosuje scentralizowany system zarządzania dostępem w celu kontroli dostępu personelu do serwerów produkcyjnych, i udziela dostępu wyłącznie ograniczonej liczbie uprawnionych pracowników. Systemy LDAP, Kerberos i wewnętrznie opracowany przez Google system wykorzystujący certyfikaty SSH mają zapewnić Google bezpieczne i elastyczne mechanizmy dostępu. Dzięki tym mechanizmom prawo dostępu do serwerów macierzystych, logów, danych i informacji nt. konfiguracji mają tylko osoby, które uzyskały zgodę na dostęp do nich. Google wymaga korzystania z niepowtarzalnych identyfikatorów użytkownika, silnych haseł, dwuskładnikowych uwierzytelnień oraz starannie monitorowanych list dostępu w celu minimalizacji ryzyka nieuprawnionego skorzystania z konta. Prawa dostępu są przyznawane i zmieniane na podstawie: zakresu obowiązków uprawnionego personelu; wymogów wynikających z obowiązków służbowych, które należy wykonać w celu wykonania uprawnionych zadań; oraz w niezbędnym zakresie. Przyznawanie i zmiana praw dostępu muszą również być zgodne z wewnętrznymi politykami i szkoleniami Google w zakresie dostępu do danych. Udzielone zgody na dostęp są zarządzane przy użyciu narzędzi do zarządzania przepływem pracy, które rejestrują wszystkie zmiany na potrzeby ew. kontroli. Również dostępy do systemów są rejestrowane na potrzeby ew. kontroli. W przypadkach gdy do uwierzytelniania stosuje się hasła (np. podczas logowania do stacji roboczych), wdrażane są polityki w zakresie haseł, które spełniają standardy nie mniej rygorystyczne od standardów ogólnie obowiązujących w branży. Standardy te przewidują ograniczenia ponownego użycia tego samego hasła oraz wymagania dotyczące minimalnej siły hasła.

3. Dane

(a) Przechowywanie, izolowanie i uwierzytelnianie danych.

Google przechowuje dane w obiektach użytkowanych przez wielu najemców, na serwerach należących do Google. Dane, bazy danych usług podmiotu przetwarzającego oraz architektura systemu plików są replikowane między wieloma, geograficznie rozproszonymi centrami danych. Google logicznie izoluje dane każdego klienta. W celu zwiększenia jednolitego bezpieczeństwa danych stosuje się system centralnego uwierzytelniania w odniesieniu do wszystkich usług podmiotu przetwarzającego.

(b) Dyski trwale wycofane z użytku oraz Wytyczne w zakresie niszczenia danych.

Niektóre dyski zawierające dane mogą mieć problemy z wydajnością, wykazywać błędy lub cierpieć na awarie sprzętowe, które skutkują koniecznością wycofania ich z użytku („**dyski trwale wycofane z użytku**"). Każdy dysk trwale wycofany z użytku poddawany jest serii procedur niszczenia danych („**Wytyczne w zakresie niszczenia danych**"), zanim opuści teren pomieszczeń Google w celu ponownego wykorzystania lub zniszczenia. Dyski trwale wycofane z użytku są czyszczone z danych w ramach wieloetapowej procedury i poddawane weryfikacji po jej ukończeniu przez co najmniej dwóch, niezależnych kontrolerów. Wyniki czyszczenia danych są rejestrowane wraz z numerem seryjnym dysku trwale wycofanego z użytku na potrzeby ich lokalizacji i monitoringu. I w końcu wyczyszczony z danych dysk trwale wycofany z użytku jest wydawany do magazynu w celu ponownego wykorzystania lub wdrożenia. Jeżeli awaria uniemożliwia wyczyszczenie danych z dysku trwale wycofanego z użytku, jest on przechowywany bezpiecznie do czasu, gdy może on zostać fizycznie zniszczony. Każdy obiekt jest poddawany regularnym kontrolom w celu sprawdzenia, czy stosowane są w nim Wytyczne w zakresie niszczenia danych.

4. Bezpieczeństwo personelu

Od personelu Google oczekuje się zachowania i postępowania w sposób zgodny z wytycznymi spółki w zakresie ochrony poufności, etyki w biznesie, właściwego wykorzystania sprzętu oraz standardów zawodowych. Google prowadzi zasadnie właściwe badania przeszłości i weryfikacje tożsamości personelu w zakresie dopuszczalnym prawem i zgodnie z mającymi zastosowanie przepisami prawa pracy i regulacjami ustawowymi.

Od personelu wymaga się podpisania umowy o zachowaniu poufności oraz poświadczenia otrzymania i zobowiązania do stosowania się do polityk Google w zakresie ochrony poufności i prywatności. Personel przechodzi szkolenie w zakresie bezpieczeństwa. Personel przetwarzający dane osobowe klienta jest zobowiązany spełnić dodatkowe wymagania stosowne do ich roli. Personel Google nie przetwarza danych osobowych klienta bez uprawnienia.

5. Bezpieczeństwo u podwykonawców przetwarzania

Przed nawiązaniem współpracy z podwykonawcą przetwarzania Google przeprowadza kontrolę praktyk w zakresie bezpieczeństwa i ochrony prywatności stosowanych przez podwykonawcę przetwarzania w celu zapewnienia, aby podwykonawca przetwarzania zapewniał poziom bezpieczeństwa i ochrony prywatności odpowiedni do jego dostępu do danych i zakresu usług, jakie są mu zlecane. Po przeprowadzeniu przez Google oceny ryzyk, jakie stwarza podwykonawca przetwarzania, i pod warunkiem spełnienia wymagań określonych w Punkcie 11.3 (Wymagania w zakresie korzystania z usług podwykonawców przetwarzania), podwykonawca przetwarzania jest zobowiązany podpisać odpowiednią umowę dotyczącą bezpieczeństwa, zachowania poufności i prywatności.