

# Google 広告データ処理規約 (Google Ads Data Processing Terms)

Google 及び本規約に同意いただいた相手方当事者（以下、「**お客様**」といいます。）は、データ処理者サービスの提供に関する契約（以下、その時々における変更を含め、「**本契約**」といいます。）を締結しています。

以下の本Google 広告データ処理規約（以下、別紙とあわせて「**本データ処理規約**」といいます。）は、Google とお客様の間で締結され、本契約を補足するものです。本データ処理規約は、本規約効力発生日をもって効力が生じ、同日以降、その目的事項に関連してそれまでに適用されていた規約（データ処理者サービスに関連するデータ処理に関する変更契約及びデータ処理に関する覚書を含みます。）に置き換わります。

あなたが、お客様に代わって本データ処理規約を承諾される場合には、あなたは、次の事項を保証するものとします：(a) ご自身が、お客様を本データ処理規約に拘束する完全な法的権限を有すること；(b) ご自身が、本データ処理規約を読み、理解していること；及び(c) ご自身が、お客様を代表して本データ処理規約に同意すること。あなたにお客様を拘束する法的権限がない場合には、本データ処理規約を承諾しないでください。

## 1. はじめに

本データ処理規約は、欧州データ保護法及び一定の欧州以外のデータ保護法に関連する一定のデータの処理に関する当事者間の合意の内容を定めています。

## 2. 定義及び解釈

2.1 本データ処理規約において、以下の文言及び表現の意味内容は、以下のとおりとします。

「**追加プロダクト**」とは、Google 又は第三者が提供するプロダクト、サービス若しくはアプリケーションであって、(a) データ処理者サービスの一部ではなく；かつ(b) データ処理者サービスのユーザー インターフェース内での使用のためにアクセス可能であるか、その他の形でデータ処理者サービスと統合されているものをいいます。

「**欧州以外のデータ保護法に関する追加規約**」とは、別紙3で参照される追加の規約であって、一定の欧州以外のデータ保護法に関連した一定のデータの処理に適用される規約に関する両当事者の合意を反映するものをいいます。

「**充分性認定国**」とは、以下に定めるものをいいます：

- EUのGDPRに従って処理されるデータについて： EEA、又はEUのGDPRに基づく充分性認定を受けている国若しくは地域；
- イギリスのGDPRに従って処理されるデータについて： イギリス、又はイギリスのGDPR及び2018年データ保護法に基づく充分性認定を受けている国若しくは地域、並びに/又は
- スイスのFDPAに従って処理されるデータについて： スイス、又は(i) スイス連邦データ保護・情報コミッショナーによって公表される法律により十分な保護水準が確保されている国家の一覧に掲載されているか、若しくは(ii) スイスのFDPAに基づきスイス連邦評議会による充分性認定を受けている国若しくは地域。

「**代替移転ソリューション**」とは、欧州データ保護法に従った個人データの第三国への適法な移転を可能にする、SCCs以外のソリューション（例えば、参加法人が充分性認定を受けていることが認められているデータ保護フレームワークなど）をいいます。

「**お客様個人データ**」とは、Google がお客様のために、Google の提供するデータ処理者サービスにおいて処理する個人データをいいます。

「**お客様SCCs**」とは、場合により、SCCs (Controller-to-Processor)、SCCs (Processor-to-Controller)、及び/又はSCCs (Processor-to-Processor)をいいます。

「**データ インシデント**」とは、Google によって管理され又はその他コントロールされているシステム上のお客様個人データに関する偶発的若しくは不法な破壊、紛失、改ざん、不正な開示又はアクセスにつながるGoogle のセキュリティの侵害をいいます。このデータ インシデントには、不正なログインの試行、ピン、ポートスキャン、DoS攻撃及びその他ファイアウォール又はネットワークシステムに対するネットワーク攻撃など、お客様個人データのセキュリティに脅威を与えない、成功しなかった試行や活動は含まれません。

「**データ主体ツール**」とは、データ主体において利用可能なツール（もしあれば）であり、これによって、お客様個人データに関するデータ主体からの一定の請求に対して、Google 法人が直接的に、標準化された方法により対応することができるもの（例えば、オンライン広告のセッティング又はオプトアウトブラウザプラグイン）をいいます。

「**EEA**」とは、欧州経済領域をいいます。

「**EU の GDPR**」とは、個人情報の処理及び個人情報の自由な移動に対する自然人の保護を目的として、EUデータ保護指令 (Directive 95/46/EC) に代わり、2016年4月27日に欧州議会及び理事会によって採択されたEU一般データ保護規則 (規則(EU)2016/679) をいいます。

「**欧州データ保護法**」とは、場合により(a) GDPR及び/又は(b) スイスのFDPAをいいます。

「**欧州の法令**」とは、(a) EU 又は EU 加盟国の法令 (EU の GDPR がお客様個人データの処理に適用される場合)、及び (b) イギリス又はイギリスの一部の法令 (イギリスの GDPR がお客様個人データの処理に適用される場合) をいいます。

「**GDPR**」とは、(a) EU の GDPR 及び/又は (b) イギリスの GDPR をいいます。

「**Google**」とは、本契約においてお客様の相手方となるGoogle 法人をいいます。

「**Google 法人**」とは、Google LLC (旧称Google Inc.)、Google Ireland Limited、並びに直接又は間接に Google LLC を支配するか、同社により支配されるか、同社と共通の支配下にある事業体をいいます。

「**指示**」は、5.2条 (お客様の指示) において当該用語に与えられた意味を有します。

「**ISO27001認証**」とは、ISO/IEC 27001:2013又はこれと同等のデータ処理者サービスに関する認証をいいます。

「**新規処理委託先**」は、11.1条 (処理委託先への委託についての同意) において当該用語に与えられた意味を有します。

「**欧州以外のデータ保護法**」とは、EEA、スイス及びイギリス以外において有効なデータ保護又はプライバシーに関する法律をいいます。

「**通知メールアドレス**」とは、本データ処理規約に関するGoogle からのお知らせを受け取るために、データ処理者サービスのユーザーインターフェース又はその他Google が提供する方法を經由してお客様が指定したメールアドレスをいいます。

「**データ処理者サービス**」とは、[business.safety.google/adsservices](#)に掲載される該当するサービスをいいます。

「**SCCs**」とは、場合により、お客様SCCs及び/又はSCCs (EU Processor-to-Processor, Google Exporter) をいいます。

「**SCCs (Controller-to-Processor)**」とは、[business.safety.google/adsprocessor/terms/sccs/eu-c2p](#)に掲載される規約をいいます。

「**SCCs (Processor-to-Controller)**」とは、[business.safety.google/adsprocessor/terms/sccs/eu-p2c](#)に掲載される規約をいいます。

「**SCCs (Processor-to-Processor)**」とは、[business.safety.google/adsprocessor/terms/sccs/eu-p2p](#)に掲載される規約をいいます。

「SCCs (Processor-to-Processor, Google Exporter)」とは、[business.safety.google/adsprocessor/terms/sccs/eu-p2p-intra-group](https://business.safety.google/adsprocessor/terms/sccs/eu-p2p-intra-group)に掲載される規約をいいます。

「セキュリティ文書」とは、ISO 27001認証の証明書及びGoogle がデータ処理者サービス上利用可能とするその他セキュリティに関する証明書又は文書をいいます。

「セキュリティ措置」とは、7.1.1条（Google のセキュリティ措置）において定められているものをいいます。

「処理委託先」とは、本データ処理規約に従って、データ処理者サービス及びこれに関連するテクニカルサポートの提供を目的として、お客様個人データへのアクセス及びその処理を行うことを許諾された第三者をいいます。

「監督機関」とは、(a) 欧州の GDPR で定義されている「監督機関」並びに/又は (b) イギリスの GDPR 及び/若しくはスイスのFDPAで定義されている「コミッション」をいいます。

「スイスのFDPA」とは、1992年6月19日の（スイスの）連邦データ保護法をいいます。

「本期間」とは、本規約効力発生日から、本契約に基づくGoogle によるデータ処理者サービスの提供の終了までの期間をいいます。

「本規約効力発生日」とは、場合により次のいずれかをいいます：

- (a) 2018年5月25日（同日以前に、お客様が本データ処理規約を承諾するためにクリックしたか、両当事者がその他の方法により当該規約に合意した場合）；又は
- (b) お客様が本データ処理規約を承諾するためにクリックしたか、両当事者がその他の方法により当該規約に合意した日（かかる日が、2018年5月25日より後である場合）。

「イギリスの GDPR」とは、イギリスの2018年欧州連合離脱法に基づき、欧州の GDPR を修正しイギリスの法令に組み込んだもの、及び同法に基づく適用ある二次的な法律をいいます。

- 2.2 本データ処理規約において用いられる「データ管理者」（controller）、「データ主体」（data subject）、「個人データ」（personal data）、「処理」（processing）、「データ処理者」（processor）は、いずれも GDPR において定められた意味を有し、「データ輸入者」（data importer）及び「データ輸出者」（data exporter）は、該当するSCCsにおいて定められた意味を有します。
- 2.3 「含む」及び「含んでいる」とは、「限定なく含んでいる」ことを意味します。本データ処理規約中の例は、あくまで例示であり、特定の概念の唯一の例ではありません。
- 2.4 本データ処理規約において言及されている法的枠組み、法令その他の制定法は、改正又は再制定があった場合、最新のものを指すものとします。
- 2.5 本データ処理規約の翻訳版と英語版との間に齟齬がある範囲において、英語版が適用されるものとします。

## 3. 本データ処理規約の期間

本データ処理規約は、本規約効力発生日をもって効力が生じます。本契約が解除されたか、期間が満了したかにかかわらず、本データ処理規約は、Google が本データ処理規約において定めるとおりすべてのお客様個人データを削除するときまで効力を有し続け、かかる時点をもって自動的に失効するものとします。

## 4. 本データ処理規約の適用

### 4.1 欧州データ保護法の適用

第5条（データの処理）乃至12条（Google へのお問合せ、処理記録）は、データ保護法がお客様個人データの処理に適用される限度で適用され、例えば、以下の例で適用されます。

- (a) 当該処理がEEA 若しくはイギリス内におけるお客様の組織の活動にかかるものである場合、及び/又は
- (b) お客様個人データがEEA 若しくはイギリス内におけるデータ主体に関する個人データであり、かつ、その処理がEEA 若しくはイギリス内にいる者への商品若しくはサービスの提供又はEEA 若しくはイギリス内にいる者の行動のモニタリングに関するものである場合

### 4.2 データ処理者サービスへの適用

本データ処理規約は、両当事者が本データ処理規約に合意したデータ処理者サービスのみに適用されます（例えば、(a) お客様が本データ処理規約を承諾するためにクリックしたデータ処理者サービス；又は(b) 本契約が参照により本データ処理規約を組み込んでいる場合に、本契約の対象となるデータ処理者サービス）。

### 4.3 欧州以外のデータ保護法に関する追加規約の組み込み

欧州以外のデータ保護法に関する追加規約は、本データ処理規約を補足するものとします。

## 5. データの処理

### 5.1 役割及び遵守並びに承認。

#### 5.1.1 データ処理者及びデータ管理者の責任

両当事者は、次の事項を確認し、合意するものとします。

- (a) 別紙1が、お客様個人データの処理の対象及び詳細を規定していること。
- (b) Google が、欧州データ保護法に基づくお客様個人データのデータ処理者であること。
- (c) お客様は、欧州データ保護法にしたがい、同法に基づくお客様個人データのデータ管理者又はデータ処理者に該当すること。
- (d) 各当事者は、お客様個人データの処理に関し、欧州データ保護法に基づき自らに課される義務を遵守すること。

#### 5.1.2 データ処理者であるお客様

お客様がデータ処理者である場合において：

- (a) お客様は、関連するデータ管理者が、(i) 指示、(ii) Google をもう一つのデータ処理者としてお客様が任命すること、及び(iii) 11条（処理委託先）に記載される処理委託先にGoogle が委託することを承認していることを継続的に保証するものとします。
- (b) お客様は、5.4条（指示通知）、7.2.1条（インシデント通知）、11.4条（処理委託先の変更に異議を唱える機会）、又はSCCsを参照する条項に基づきGoogle によって提供される通知に関連するデータ管理者に直ちに転送するものとします。
- (c) お客様は、7.4条（セキュリティ認証）、10.5条（データセンター情報）及び11.2条（処理委託先に関する情報）に基づきGoogle によって利用可能とされる情報に関連するデータ管理者に対して利用可能とできるものとします。

### 5.2 お客様の指示

本データ処理規約を締結することにより、お客様は、Google に対し、適用される法令にのみ従って、お客様個人データを、(a)データ処理者サービス及び関連する技術的サポートを提供するために、(b)お客様によるデータ処理者サービス（データ処理者サービスの設定及びその他の機能を含む）及び関連する技術的サポートの利用を通じてより詳細に特定される通りに、(c)本データ処理規約を含む本契約の形で規定されている通りに、かつ(d)お客様によってなされるその他の書面による指示であって、本データ処理規約の目的において指示にあたりGoogle によって認識されるものにおいて詳細が記載される通りに処理することを指示するものとします（以下、「指示」と総称します。）。

### 5.3 Google による指示の遵守

Google は、欧州の法令によって禁止されていない限り、指示を遵守します。

#### 5.4 指示通知

Google は、Google の見解において、(a) 欧州の法令により Google が指示に従うことを禁止されているか、(b) 指示が欧州データ保護法に沿ったものでないか、又は(c) Google が指示に従うことができないと判断される場合には、直ちにお客様に通知しますが、それぞれの場合において、かかる通知が欧州の法令によって禁止されているときは、この限りではありません。本5.4条（指示通知）は、本契約の別の定めにおける各当事者の権利義務を軽減するものではありません。

#### 5.5 追加プロダクト

お客様が追加プロダクトを利用する場合には、当該追加プロダクトのデータ処理者サービスとの相互運用のために必要となる範囲で、データ処理者サービスにおいて、当該追加プロダクトがお客様個人データにアクセスすることが許可されるものとします。正確を期すため、本データ処理者規約は、個人データが追加プロダクトとの間で送受信されることを含め、お客様が利用する追加プロダクトの提供に関連した個人データの処理には適用されないことを付記します。

## 6. データの削除

#### 6.1 本期間中の削除

##### 6.1.1 削除機能のあるデータ処理者サービス

Google は、本期間中、以下に掲げる場合には、合理的に実行可能な限り速やかに、最大180日間以内に、システムからそれらのお客様個人データを削除するものとします。ただし、欧州の法令により保管が必要な場合を除きます。

- (a) データ処理者サービスの機能にお客様がお客様個人データを削除するオプションが含まれている場合
- (b) お客様が、特定のお客様個人データを削除するためにデータ処理者サービスを利用する場合
- (c) お客様によって削除されたお客様個人データを（例えば「ゴミ箱」から）復元させることが不可能な場合

##### 6.1.2 削除機能のないデータ処理者サービス

本期間中、データ処理者サービスにお客様がお客様個人データを削除するオプションが含まれていない場合には、Google は、以下に従うものとします：

- (a) データ処理者サービスの性質及び機能を考慮の上、欧州の法令により保管が必要な場合を除き、可能な限り、お客様からの個人データの削除を促進することの合理的な請求；及び
- (b) [policies.google.com/technologies/ads](https://policies.google.com/technologies/ads)に記載されるデータ保持実務。

Google は、6.1.2条(a)に基づくデータの削除について、（Google の合理的な費用に基づく）料金を請求することができます。Google は、かかるデータの削除に先立って、お客様に対し、当該料金の詳細及びその計算の根拠を提供します。

#### 6.2 本期間満了時の削除

お客様は、Google に対し、適用される法令に従って、本期間終了時においてGoogle のシステムからすべての残存するお客様個人データ（既存の複製データを含む）を削除するよう指示します。Google は、欧州の法令により保存が要求される場合を除き、実行可能な限り速やかに、最大180日間以内に、この指示に従うものとします。

## 7. データセキュリティ

#### 7.1 Google のセキュリティ措置及び支援

##### 7.1.1 Google のセキュリティ措置

Google は、別紙2に記載されているとおり、偶発的又は不法な破壊、紛失、改ざん、不正な開示又はアクセスからお客様個人データを保護するための技術的及び組織的措置を実行し、維持するものとします（以下、「**セキュリティ措置**」といいます。）。別紙2に記載されるとおり、セキュリティ措置には、(a) 個人データを暗号化するため、(b) Google のシステム及びサービスの秘密保持、インテグリティ、アベイラビリティ及び回復力を継続的に確保するため、(c) インシデント発生後に個人データへのアクセスを適時に復旧するため、また(d) 有効性の定期的な検査のための措置が含まれます。Google は、セキュリティ措置を随時更新又は修正することができますが、これによりデータ処理者サービスの全体のセキュリティを低下させないものとします。

##### 7.1.2 アクセス及びコンプライアンス

Google は、(a) 自社の従業員、契約業者及び処理委託先に対して、指示に応じるために厳に必要な範囲でのみ、お客様個人データにアクセスする権限を与え、(b) 自社の従業員、契約業者及び処理委託先が、それらの者の業務の範囲に適用される範囲でセキュリティ措置を遵守するよう徹底するための適切な手順を実施し、かつ(c) Google は、お客様個人データの処理を許可されたすべての者に、機密保持を誓約させ、又は適切な法令に基づく機密保持義務を負わせるようにします。

##### 7.1.3 Google のセキュリティ支援

Google は、（Google が利用可能なお客様個人データ及び情報の処理の性質を考慮の上）以下に掲げる事項により、お客様が、お客様（又は、お客様が処理者である場合には、関連するデータ管理者）のGDPR32条から34条に基づく義務を含む、個人データのセキュリティ及び個人データの侵害に関するお客様（又は、お客様が処理者である場合には、関連するデータ管理者）の義務の遵守を確実にできるよう支援します。

- (a) 7.1.1条（Google のセキュリティ措置）に基づくセキュリティ措置の実行及び維持
- (b) 7.2条（データ インシデント）に定める条件の遵守
- (c) 7.5.1条（セキュリティ文書の検証）に基づくセキュリティ文書及び本データ処理規約に含まれる情報のお客様への提供

#### 7.2 データ インシデント

##### 7.2.1 インシデント通知

Google がデータ インシデントを認識した場合、Google は、(a) お客様に対し、データ インシデントが発生した旨を速やかにかつ不当な遅滞なく通知し、かつ(b) 損害を最小限にし、お客様個人データを保護するための、合理的な措置を速やかに講じます。

##### 7.2.2 データ インシデントの詳細

7.2.1条に基づく通知（インシデント通知）では、影響を受けるお客様のリソース、データ インシデントに対応し、潜在的リスクを緩和するためにGoogle が講じたか、講じる予定の対策、Google がお客様に推奨するデータ インシデントに対応する方法（もしあれば）、及び詳細な情報が得られる連絡先の詳細も含めて、データ インシデントの性質を記載いたします。それらすべての情報を同時に提供するのが不可能である場合には、Google の当初の通知には、その時点で提示可能な情報が記載され、詳細な情報は、提示可能となり次第、不当な遅延なく提供されるものとします。

##### 7.2.3 通知の発信

Google は、上記データ インシデントの通知を通知メールアドレスに発信するか、又はGoogle の裁量により（お客様が通知メールアドレスを提供していない場合などに）他の直接的な連絡方法（電話又は直接対面する方法など。）で通知いたします。お客様は、通知メールアドレスを提供し、かつ確実に通知メールアドレスが現在のものであり、かつ有効であるようにすることに単独で責任を負うものとします。

##### 7.2.4 第三者通知

お客様は、お客様に適用される事故通知に関する法律を遵守すること、及び、データ インシデントに関する第三者への通知義務を履行することについて単独で責任を負います。

##### 7.2.5 Google の過失承服の不存在

7.2条（データ インシデント）に基づくデータ インシデントに対するGoogle からの通知または返答は、データ インシデントに関していかなる過失や責任をもGoogle が認めたものとは解されません。

## 7.3 お客様のセキュリティ上の責任と評価

### 7.3.1 お客様のセキュリティ上の責任

7.1条（Googleのセキュリティ措置及び支援）及び7.2条（データインシデント）を変更しない範囲で、次の事項に同意します。

- (a) お客様が以下の各号を含めたデータ処理者サービスの利用について責任を負うこと。
  - (i) お客様個人データに関するリスクに対して適切なセキュリティのレベルを確保するため、データ処理者サービスを適切に利用すること
  - (ii) お客様がデータ処理者サービスにアクセスするために使用するアカウント認証のために要求される情報、システム及びデバイスを保護すること
- (b) お客様がGoogleのシステム又は処理委託先のシステム以外の場所にお客様個人データを保管又は移転することを選択した場合、Googleは、かかるお客様個人データを守る義務を負わないこと。

### 7.3.2 お客様のセキュリティ評価

お客様は、7.1.1条（Googleのセキュリティ措置）に記載されている、Googleによって実行、維持されるセキュリティ措置が、最先端の技術、実施コストやお客様個人データ及び各個人に対するリスクの処理の性質、範囲、背景や目的を考慮の上、お客様個人データに関するリスクに対して適切なレベルのセキュリティを提供していることにつき承諾し、同意するものとします。

## 7.4 セキュリティ認証

セキュリティ措置の継続的な有効性を評価し、その確保に役立てるため、Googleは、ISO 27001認証を維持するものとします。

## 7.5 コンプライアンスの検証と監査

### 7.5.1 セキュリティ文書の検証

本データ処理規約に基づく義務をGoogleが遵守していることを実証するため、Googleは、お客様がセキュリティ文書を検証することができるようにします。

### 7.5.2 お客様の監査の権利

- (a) Googleは、Googleが本データ処理規約に基づく義務を遵守していることを検証するため、7.5.3条（監査のための追加ビジネス条項）にしたがい、お客様又はお客様が任命した第三者監査人が監査（調査を含む）を実施することを認めます。監査中、Googleは、かかる遵守を証明するために必要な一切の情報を閲覧可能とし、7.4条（セキュリティ認証）及び7.5条（コンプライアンスの検証と監査）に記載されている通り、監査に協力いたします。
- (b) SCCsが、10.2条（制限される移転）に基づき適用される場合、Googleは、7.5.3条（監査のための追加ビジネス条項）にしたがい、お客様（又はお客様が任命した第三者監査人）が、SCCsに記載される監査を実施することを認め、監査中、当該SCCsにより要求されるすべての情報を閲覧可能とします。
- (c) お客様はまた、Googleが本データ処理規約に基づく義務を遵守していることを検証するため、（第三者監査人による監査の結果を反映した）ISO 27001認証のために発行された証明書を検証する方法により、監査を実施することができます。

### 7.5.3 監査のための追加ビジネス条項

- (a) お客様は、12.1条（Googleへのお問合せ）に記載されている方法で、7.5.2(a)条又は7.5.2(b)条に基づく監査のリクエストを送るものとします。
- (b) 7.5.3(a)条又は7.5.2(b)条に基づくリクエストをGoogleが受領した場合、Googleとお客様は、7.5.2(a)条に基づく監査の合理的な開始日、範囲及び期間並びにかかる監査に適用されるセキュリティ及び機密性の管理について、事前に協議の上合意します。
- (c) Googleは、7.5.2(a)条又は7.5.2(b)条に基づく監査のための（Googleの合理的な費用に基づく）料金を請求することができます。Googleは、監査に先立って、お客様に対し請求される料金及びその根拠となった計算式の詳細について提供します。お客様は、お客様が任命した第三者監査人によって請求される監査を実施するための料金について責任を負います。
- (d) Googleは、7.5.2(a)条又は7.5.2(b)条に基づく監査を実施するためにお客様によって任命された第三者監査人が、Googleの合理的な見解として、相応の資格を有していない、独立していない、Googleの競合他社である又はその他明らかに不適格である場合、当該第三者監査人について異議を申し立てることができます。かかる異議が申し立てられた場合、お客様は、他の第三者監査人を選任するか、自らかかる監査を行うものとします。
- (e) 本データ処理規約は、Googleに対して、以下の各号に掲げる情報について、お客様又はその第三者監査人への情報開示又はアクセス許可を何ら要求するものではありません。
  - (i) Google法人の他のお客様に関するデータ
  - (ii) Google法人内部の会計又は財務情報
  - (iii) Google法人の営業秘密
  - (iv) Googleの合理的見解として、（A）Google法人のシステム又は施設のセキュリティを脅かす可能性のある情報、又は（B）Google法人に、欧州データ保護法上の義務違反又はお客様若しくは第三者に対するセキュリティ及び/若しくはプライバシーの義務違反を生じさせる可能性のある情報
  - (v) お客様又はその第三者監査人が欧州データ保護法に基づくお客様の義務の誠実な履行以外の理由でアクセスを求める情報

## 8. 影響評価と相談

Googleは、GDPRの35条及び36条に従ったお客様又は関連するデータ管理者の義務（該当する場合）を含む、データ保護の影響評価や事前相談に関して、（処理の性質やGoogleが取得できる情報を考慮して）以下の各号の方法によって、お客様がお客様（又は、お客様が処理者である場合には、関連するデータ管理者）の義務遵守を確保することを支援します。

- (a) 7.5.1条（セキュリティ文書の検証）に従って、セキュリティ文書を提供すること
- (b) 本契約（本データ処理規約を含みます。）に含まれる情報を提供すること
- (c) Googleの通常の運用にしたがい、データ処理者サービスの性質やお客様個人データの処理に関係するその他の資料（例、ヘルプセンター資料など）を提供又は入手可能にすること

## 9. データ主体の権利

### 9.1 データ主体からの請求への対応

Googleがデータ主体からお客様個人データに関する請求を受けた場合には、お客様は、次の事項を行う権限をGoogleに与え、Googleは、お客様に対してここに次の事項を通知します。

- (a) データ主体ツールの標準機能に従って、直接対応すること（当該請求がデータ主体ツールを介して行われたとき）。
- (b) データ主体に対して、お客様へ当該請求を提出するように助言すること（当該請求がデータ主体ツールを介さずに行われたとき）。この場合、お客様が、当該請求に返答する責任を有することになります。

### 9.2 Googleによるデータ主体の要求の支援

GDPR第3章に基づきデータ主体の権利を実現するための請求に対応するお客様（又は、お客様が処理者である場合には、関連するデータ管理者）の義務を果たすにあたって、Googleは、あらゆる場合において、お客様個人データを処理することの特質及びGDPR第11条（適用される場合）を考慮した上で、以下の方法でお客様

を支援します。

- (a) データ処理者サービスの機能の提供
- (b) 9.1条（データ主体からの請求への対応）に規定される責任を果たすこと
- (c) 利用可能なデータ主体ツールの作成（データ処理者サービスに適用される場合）

### 9.3 修正

お客様が、お客様個人データが不正確であるか、最新でないと認識した場合には、お客様は、欧州データ保護法により要求されるときには、（該当する場合において）データ処理者サービスの機能を用いて行う場合を含め、かかるデータの修正や削除に責任を負うものとします。

## 10. データの移転

### 10.1 データの保管及び処理の施設

本10条（データの移転）のその他の規定を前提として、Google は、Google 又はその処理委託先が管理している施設のある国において、お客様個人データを保管及び処理することができます。

### 10.2 制限される移転

欧州データ保護法によって、十分性認定国におけるお客様個人データの処理、又はかかる国への当該データの移転（以下、「**許容される移転**」といいます。）のために、SCCs又は代替移転ソリューションは要求されていないことを、両当事者は確認するものとします。お客様個人データの処理が、許容される移転ではない移転を伴うものであり、欧州データ保護法が当該移転に適用される場合（以下、「**制限される移転**」といいます。）において：

- (a) Google が、制限される移転について、代替移転ソリューションを採用する場合には、Google は、当該ソリューションにつきお客様に通知し、かかる移転が当該代替移転ソリューションに従って行われるように徹底し；かつ/あるいは
- (b) Google が、制限される移転について、代替移転ソリューションを採用しない場合、またはGoogle が制限される移転について代替移転ソリューションの採用を続けなことをお客様に通知した場合において：
  - (i) Google の所在地が十分性認定国内にあるときは：
    - (A) SCCs (Processor-to-Processor, Google Exporter) が、Google から処理委託先へのすべての制限される移転について適用され；
    - (B) また、お客様の所在地が十分性認定国内にないときは、SCCs (Processor-to-Controller) が、（お客様がデータ管理者及び/又はデータ処理者であるかにかかわらず）Google とお客様との間の制限される移転について適用されます。
  - (ii) Google の所在地が十分性認定国内にないときは：

SCCs (Controller-to-Processor) 及び/又は SCCs (EU Processor-to-Processor) が、（お客様がデータ管理者及び/又はデータ処理者であるか否かによって）お客様とGoogleとの間の制限される移転について適用されます。

### 10.3 補足的な措置及び情報

Google は、お客様に、制限される移転に関連する情報を提供するものとし、これには、7.5.1条（セキュリティ文書の検証）、別紙2（セキュリティ対策）、並びにデータ処理者サービスの特質及びお客様個人データの処理に関するその他の資料（例えば、ヘルプセンターの掲載記事）に記載されるとおり、お客様個人データを保護するための補足的な措置に関する情報が含まれます。

### 10.4 終了

お客様が、自らによるデータ処理者サービスの現時点の利用又は予定された利用に基づき、場合により代替移転ソリューション及び/又はSCCsによって、お客様個人データについて適切な保護策が提供されないと結論付けた場合には、お客様は、Google に対して書面で通知することにより、自己都合により本契約を直ちに終了できるものとします。

### 10.5 データセンター情報

Google のデータセンターの場所に関する情報については、[www.google.com/about/datacenters/locations/](http://www.google.com/about/datacenters/locations/)をご覧ください。

## 11. 処理委託先

### 11.1 処理委託先への委託についての同意

お客様は、11.2条（処理委託先に関する情報）に記載されるURLにおいて本規約効力発生日に掲載される事業者が処理委託先として委託を受けることについて明確に承認します。さらに、11.4条（処理委託先の変更に異議を唱える機会）を損なうことなく、お客様は、その他の第三者が処理委託先として（以下、「**新規処理委託先**」といいます。）委託を受けることについて、包括的な承認を与えるものとします。

### 11.2 処理委託先に関する情報

処理委託先に関する情報については、[business.safety.google/adssubprocessors](http://business.safety.google/adssubprocessors)をご覧ください。

### 11.3 処理委託先への委託についての要件

処理委託先に委託する場合には、Google は以下のことを行います。

- (a) 書面による契約によって、以下の事項を実現します。
  - (i) 処理委託先は、委託された義務の遂行に必要な限度でのみ、お客様個人データを入手及び利用し、また、（本データ処理規約を含む）本契約に従ってこれらを行います。
  - (ii) お客様個人データの処理に欧州データ保護法が適用される場合には、本データ処理規約中のデータ保護義務（該当する場合において、GDPR第28条第3項で参照されるとおり）が処理委託先に課されます。
- (b) 処理委託先へ委託されたすべての義務及び処理委託先のすべての行為及び過失について、完全な責任を保持します。

### 11.4 処理委託先の変更に異議を唱える機会

- (a) 本期間中に新規処理委託先への委託が行われた場合には、Google は、新規処理委託先がお客様個人データを処理する少なくとも30日前までに、お客様に対して、通知メールアドレスにEメールを送信することにより当該委託について（該当する処理委託先の名称及び所在地、並びに実施される業務内容を含みます。）連絡します。
- (b) お客様は、Google に対する書面による通知をもって、自己都合により直ちに本契約を終了することにより、新規処理委託先に異議を唱えることができます。ただし、お客様が、11.4条(a)に記載されるとおり新規処理委託先の委託について通知を受けてから90日以内にかかる通知を行うことを条件とします。

## 12. Google へのお問合せ、処理記録

### 12.1 Google へのお問合せ

お客様は、本データ処理規約に規定された権利の行使に関連して、[privacy.google.com/businesses/processorsupport](http://privacy.google.com/businesses/processorsupport) に記載の方法を用いるか、その他、Google から随時提供される方法によって、Google に問い合わせることができます。Google は、かかる方法によってGoogle が受け取り、本契約に基づくお客様個人データの処理に関連するお客様によるお問合せに対して迅速かつ合理的に対応するものとします。

### 12.2 Google の処理記録

Google は、GDPRにより要求されるとおり、自らの処理業務に関して、適切な文書を保持します。GDPRにより、Google は、(a) (i) Google が代表する個々のデータ処理者及び/又はデータ管理者並びに（適用される場合には）当該データ処理者又はデータ管理者の地域における代表者及びデータ保護官の、氏名及び連絡先、並びに(ii) お客様SCCsに基づき該当する場合には、お客様の監督当局を含む、特定の情報の記録を収集し維持しなければならず、(b) 当該情報を監督機関に対して利用可能にしなければならないこととされていることを、お客様は確認します。従って、お客様は、要求されかつお客様に適用される場合には、Google に対し、当該情報を、データ処理者サービスのユーザー インターフェース又はその他Google から提供される類似の方法を通じて提供し、さらに、当該ユーザー インターフェース又はその他の手段により、提供されたすべての情報が正確かつ最新であるようにします。

#### 12.3 管理者による請求

Google が12.1条に記載される方法（若しくはその他いかなる方法）により、お客様個人データの管理者であると主張する第三者から請求又は指示を受けた場合には、Google は、当該第三者に対して、お客様に連絡するよう伝えるものとします。

## 13. 責任

- (a) 本契約にアメリカ合衆国のある州の法律が適用される場合には、本契約の別の定めにかかわらず、本データ処理規約に基づく又は関連した、一方当事者からの相手方当事者への責任総額は、本契約に基づき当該当事者の責任の上限として定められる特定の金額又は支払額に基づき定める金額のうち上限の金額に限定されることとなります（よって、本契約の責任限定からの補償に関する請求についての除外は、欧州データ保護法又は欧州以外のデータ保護法に関連する本契約に基づく補償の請求には適用されません。）。
- (b) 本契約にアメリカ合衆国の州ではない法域の法律が適用される場合には、本データ処理規約に基づく又は関連した両当事者の責任は、本契約における除外及び責任限定の規定に従うものとします。

## 14. 本データ処理規約の効果

#### 14.1 優先順位

お客様SCCs、欧州以外のデータ保護法に関する追加規約、本データ処理規約のその他の条項、及び/又は本契約のその他の部分に矛盾又は不一致があった場合には、次の優先順位が適用されます。

- (a) お客様SCCs（該当する場合）
- (b) 欧州以外のデータ保護法に関する追加規約（該当する場合）
- (c) 本データ処理規約のその他の条項
- (d) 本契約のその他の部分

本契約は、本データ処理規約により修正されることを条件として、有効に存続します。

#### 14.2 SCCsの変更のないこと

本契約（本データ処理規約を含みます。）中のいかなる定めも、SCCsを変更し、若しくはSCCsと矛盾すること、又は欧州データ保護法に基づくデータ主体の基本的権利又は自由を損なうことを意図していません。

#### 14.3 管理者規約に対する影響のないこと

本データ処理規約は、データ処理者サービス以外のサービスについてのデータ管理者間の関係を反映するGoogle とお客様との間の別個の規約には影響を及ぼしません。

#### 14.4 従前のイギリス SCCs (UK SCCs)

2022年9月21日、又は本契約の効力発生日のどちらか遅い方の日付をもって、イギリスのGDPRについての移転に関するSCCsの補足条項が適用され、イギリスのGDPR及び2018年データ保護法に基づき承認され、お客様とGoogle との間で過去に締結された、いかなる標準的契約条項（以下、「従前のイギリスのSCCs」といいます。）に置き換わり、当該条項を終了させるものとします。本14.4条（従前のイギリスのSCCs）は、従前のイギリスのSCCsが効力を有していた間にこれに基づき発生した可能性のある、いずれの当事者の権利にも、いずれのデータ主体の権利にも影響を及ぼさないものとします。

## 15. 本データ処理規約の変更

#### 15.1 URLの変更

Google は、本データ処理規約において参照されるURL及び当該URLで掲載される内容を随時変更できるものとしますが、Google による変更は、以下の場合に限りです。

- (a) 15.2条(b)乃至15.2条(d)（本データ処理規約の変更）に従ったSCCsの変更、又は欧州データ保護法に基づき採用されるSCCsの新たなバージョンの組み込み（それぞれの場合において、欧州データ保護法に基づくSCCsの有効性に影響を及ぼさない方法によるものとします。）
- (b) (i) サービスの名称変更を反映させるため、(ii) 新たなサービスを追加するため、又は(iii) (x) 当該サービスを提供する全ての契約が終了している場合、若しくは(y) Google がお客様の同意を得ている場合に、サービスを削除するための、[business.safety.google/adsservices](#)における潜在的なデータ処理者サービスのリストの変更

#### 15.2 データ処理規約の変更

Google は、以下の場合、本データ処理規約の変更をすることができます。

- (a) 15.1条（URLの変更）によるものなど、本データ処理規約によって明示的に許可されている場合
- (b) 法人の名称又は組織の変更を反映する場合
- (c) 適用される法律又は規制、裁判所命令、政府の監督者又は官庁によって発されたガイダンスを遵守するために必要であるか、Google による代替移転ソリューションの採用を反映する場合
- (d) (i) データ処理者サービスの全体のセキュリティの低化を招かず、(ii) (x) 欧州以外のデータ保護法に関する追加規約の場合において、欧州以外のデータ保護法に関する追加規約の範囲内のデータを使用若しくはその他の方法で処理するGoogle の権利や、(y) 本データ処理規約のその他の規定の場合において、5.3条（Google による指示の遵守）に規定されている、Google によるお客様個人データの処理について、その範囲を拡大したりその処理に対する規制を除去したりせず、かつ、(iii) 本データ処理規約に基づくお客様の権利に対して重大かつ不利益な影響力を有しないとGoogle が合理的に決定した場合

#### 15.3 変更通知

Google が15.2条(c)又は(d)に基づき本データ処理規約を変更しようとする場合には、Google は、当該変更の効力が生じる少なくとも30日前までに（又は、適用法令、裁判所命令、若しくは政府の規制当局や機関が発するガイダンスに従うために必要となるそれより短い期間中に）、(a) 通知メールアドレス宛てのEメールの送信、又は(b) データ処理者サービスのユーザーインターフェースでのお客様への注意喚起のいずれかの方法によりお客様に連絡します。お客様が当該変更が不服である場合には、お客様は、Google による当該変更の通知を受けてから90日以内にGoogle に書面による通知を行うことにより、自己都合により本契約を直ちに終了することができます。

## 別紙 1 本データ処理の対象と細目

#### 対象

Google によるお客様へのデータ処理者サービス及びその他関連する技術サポートの提供

## 本処理の期間

本期間及び本期間の終了から、本データ処理規約にしたがい、Google によってお客様個人データが削除されるまでの期間

## 本処理の性質と目的

Google は、お客様へデータ処理者サービス及びその他関連する技術サポートを提供するという目的のために、本処理データ規約に従って、お客様個人データを処理します（データ処理者サービス及び指示に適用される、収集、記録、整理、構成、保管、修正、回収、使用、開示、組み合わせ、消去及び破壊を含みます。）。

## 個人データの種類

お客様個人データには、[business.safety.google/adsservices](https://business.safety.google/adsservices)に記載される個人データの種類が含まれる場合があります。

## データ主体のカテゴリー

お客様個人データは、以下のカテゴリーのデータ主体に関連するものとなります。

- Google が、自らによるデータ処理者サービスの提供において個人データを収集する対象とするデータ主体；及び/又は
- お客様によって、お客様の指図により、又はお客様のためにデータ処理者サービスに関連して個人データがGoogle に移転されるデータ主体

データ処理者サービスの性質により、これらのデータ主体には、(a) オンライン広告の対象とされているか、対象とされる個人、(b) Google によるデータ処理者サービスの提供に関連する特定のウェブサイト若しくはアプリケーションを閲覧した個人、及び/又は(c) お客様のプロダクト若しくはサービスの顧客やユーザーである個人が含まれる場合があります。

# 別紙2 セキュリティ対策

効力発生日より、Google は、本別紙2記載のセキュリティ対策を実施及び維持します。Google は、随時、このセキュリティ対策を改訂又は修正することができます。ただし、当該改訂及び修正は、データ処理者サービスの全体的なセキュリティを低下させるものではないものとします。

## 1. データセンターとネットワークセキュリティー

### (a) データセンター

#### インフラストラクチャー

Google は、地理的に分散されたデータセンターを保持します。Google は、全てのプロダクション データを物理的に安全なセキュリティーセンターに保管します。

#### 冗長化

インフラストラクチャー システムは、単一障害点を除去し、懸念される環境リスクの影響を最小化するように設定されています。回路、スイッチ、ネットワーク又はその他の必要な装置の二重化はこの冗長化の提供に役立ちます。データ処理者サービスは、Google が特定の種類の予防・是正管理を間断なく実行できるように設計されています。全ての環境装置及び設備は、製造者又は内部の仕様書に従った、実施ためのプロセスとその頻度について詳しく述べた予防管理手続を記録しています。データセンター装置の予防・是正管理は、記録化された手続きに従った標準的なプロセスを通じて計画されています。

#### 電力

データセンターの電力システムは、24時間、週7日間の継続運転に影響を及ぼすことなく、冗長で維持可能な状態にあるよう設定されています。ほとんどの場合、主要電源と代替電源が、それぞれ同じ容量で、データセンターにおける主要なインフラストラクチャーの構成要素に供給されます。バックアップ電源は、公共電力の電力低下、停電、過電圧、電圧不足、許容範囲を超える周波状態の間に、絶えず確実な電力保護を供給する無停電電源（UPS）バッテリーのような様々なメカニズムによって供給されます。公共電力が遮断された場合、バックアップ電源は、バックアップ発電機システムが引き継ぐまで最大で10分間、フル操業で、データセンターに一時的な電力を供給するよう設定されています。バックアップ発電機は、データセンターをフル操業で通常どおり数日間操業するために十分な緊急電力を、すぐに供給するよう自動的に始動することができます。

#### サーバー操作システム

Google サーバーは、そのビジネスに特有のサーバーへの必要性に従ってカスタマイズされた強化オペレーティング・システムを使用しています。データは、データのセキュリティ及び冗長化を増強する独自のアルゴリズムを使用しながら保存されます。Google は、データ処理者サービスを提供するために使用されるコードのセキュリティを強化し、プロダクション環境におけるセキュリティ製品の機能を高めるためのコードレビューシステムを利用しています。

#### ビジネス継続性

Google は、予期せぬ破壊や紛失から守るのに役立つため、多重のシステムでデータを複製します。Google は、そのビジネス継続性の計画・災害復旧プログラムを設定し、定期的に計画及び検査をしています。

#### 暗号化技術

Google のセキュリティポリシーにより、個人データを含むすべてのユーザー データについて、保存データの暗号化が必須とされています。データは、顧客による手続を要することなく、データセンターにおけるGoogle のプロダクション ストレージスタックにおいて、ハードウェアのレベルを含む複数のレベルでの暗号化がよく行われます。複数レイヤーでの暗号化を用いることにより、十分なまでのデータ保護がもたらされ、Google は、アプリケーションの要件に基づく最適なアプローチを選択することができます。個人データはすべて、ストレージのレベルで、通常AES256を用いて暗号化されます。Google は、データ処理者サービス全体で一貫して暗号化を実施するために、Google のFIPS 140-2認定モジュールを組み込んだ共通暗号化ライブラリを使用します。

### (b) ネットワークと通信

#### データ通信

データセンターは、通常、データセンター間での安全で迅速なデータ移転を提供するため、高速なプライベートリンクを経由して接続されます。また、Google は、データセンター間で伝送されるデータを暗号化します。これは、電子送信中に、無許可でデータが読み取られ、複製され、変更され又は除去されることを防ぐために設定されたものです。Google は、データをインターネットの標準プロトコルにより転送します。

#### 外部からの攻撃の対象

Google は、外部からの攻撃の対象を守るため、多重のネットワーク装置と侵入検知を利用します。Google は、潜在的な攻撃ベクターを考慮し、適切な専用の技術を外部との対面システムに組み入れます。

#### 侵入検知

侵入検知は、進行中の攻撃活動の手掛かりとなり、インシデントに対応するために適切な情報を提供することを目的としています。Google の侵入検知には、以下の事項を含みます。

- 予防的措置を通じて、攻撃を受ける対象の大きさや構造を的確に管理すること。
- データ入力ポイントにおいて、高度な処理能力を有する検知機能を使用すること。
- 特定の危険な状況を自動的に改善する技術を使用すること。

#### インシデント対応

Google は、セキュリティーインシデントに備えて、様々な通信経路を監視し、Google のセキュリティー担当者は、感知されたインシデントに早急に対応します。

#### 暗号化技術

Google は、HTTPS暗号（TLS接続とも呼ばれます。）を有効化します。Google のサーバーは、RSAとECDSAで署名される一時的な楕円曲線ディフィー・ヘルマン暗号鍵共有をサポートします。これらの完全前方秘匿性（PFS）の方法は、トラフィックを守り、侵害された鍵や暗号化の突破による影響を最小化することに役立ちます。

## 2. アクセス コントロール及びサイト コントロール

(a) サイトコントロール

データセンターの現地セキュリティ オペレーション

Google のデータセンターでは、1日24時間、週7日間、物理的なデータセンターのセキュリティ機能を担う現地セキュリティ オペレーションを整備しています。現地セキュリティ オペレーションの担当者は、クローズドサーキットTV (CCTV) カメラ及び全警報システムを監視するほか、定期的にデータセンターの内部及び外部のパトロールを行います。

データセンターへの立入手続

Google は、データセンターへの物理的なアクセスの許可に関する正規の手続を整備しています。データセンターは電子カードキーが必要な施設に收容されており、現地セキュリティ オペレーションチームと接続されたアラームも備えています。データセンターに立ち入る場合は誰であれ、現地セキュリティ オペレーションチームに身分証明書を示すよう求められるとともに、本人確認が求められます。許可を受けた社員、契約業者及び訪問者のみがデータセンターに立ち入ることができません。これらの施設に立ち入るための電子カードキーは、許可を受けた従業員、請負業者及び訪問者のみ交付を受けることができます。データセンターの電子カードキーの交付を受けるには、事前の書面による申請と、権限を有するデータセンター担当者の承認が必要です。これ以外の、一時的にデータセンターへの立ち入りを必要とする者は、(i) 訪問しようとする特定のデータセンター及び内部エリアについて権限を有するデータセンター担当者から事前に承認を得たうえで、(ii) 現地セキュリティ オペレーションチームにてサインインし、(iii) 自身が承認を受けていることを示す承認記録を示さなければなりません。

データセンター現地のセキュリティ デバイス

Google のデータセンターでは、システムアラームと接続された電子カードキー及び生体アクセス コントロールシステムを採用しています。このアクセス コントロールシステムは、各個人の電子カードキーを監視、記録するとともに、区画の境界ドア、荷物の発送及び受領その他の重要な領域にアクセスした日時を記録します。許可を受けていない行動及び失敗したアクセス試行はアクセス コントロールシステムによって記録され、必要に応じて調査されます。事業活動及びデータセンター全体の立入許可は、ゾーン及び個人の職務に応じて制限されています。データセンターの防火ドアに対しては警戒が実施されています。CCTVはデータセンターの内部及び外部で動作しています。CCTVは、戦略的エリア、とりわけ境界線、データセンター建物への境界ドアや荷物の発送・受領を監視できるように配置されています。現地セキュリティ オペレーションチームの担当者は、CCTVを監視、記録し、機器の制御に当たります。CCTVの設備は、データセンターに張り巡らされた安全なケーブルによって接続されています。カメラはデジタルビデオ レコーダーによって、現地の状況を1日24時間、週7日間記録しています。監視記録は活動があってから最低7日間保存されます。

(b) アクセスコントロール

インフラストラクチャー セキュリティ担当者

Google は、従業員のためのセキュリティポリシーを策定、維持しており、従業員のための研修パッケージの一環として、セキュリティ研修を必修としております。Google のインフラストラクチャー セキュリティ担当者は、Google のセキュリティ インフラストラクチャーの継続的な監視、データ処理者サービスの検査、セキュリティ事案への対応を担当しています。

アクセス コントロールと権限管理

データ処理者サービスを利用するために、お客様の管理者とユーザーの認証は、中央認証システム又はシングル サインオン システムを通じてなされる必要があります。

内部データアクセス手順とポリシー – アクセスポリシー

Google の内部データにアクセスする手順及びポリシーは、権限のない人物及び/又はシステムが個人情報処理するシステムにアクセスすることを防止するよう設計されています。Google は、(i) 許可を受けたユーザーのみが、アクセス許可を受けたデータにのみアクセスするよう、また、(ii) 処理、利用又は記録後に、個人データが許可なく読み取り、複製、改変、消去されないよう、システムを設計することを目指しています。システムはあらゆる不適切なアクセスを検知するよう設計されています。Google では、プロダクションサーバーにアクセスできる人員を管理するため、また、限定された人数の権限ある担当者のみがアクセス可能とするため、アクセスの集中管理システムを採用しております。LDAP、Kerberos及びデジタル認証を用いた独自のシステムは、安全で柔軟なアクセス メカニズムをGoogle にもたらすよう設計されています。これらのメカニズムは、サイトホストやログ、データ及び構成情報に対し、承認されたアクセス権のみを付与するよう設計されています。Google では、アカウントの不正な利用のおそれを最小化するために、一意のユーザーID、強力なパスワード、二段階認証及び慎重に監視されたアクセスリストの使用を要求しています。アクセス権の付与又は変更は、正当な職務権限、正当な業務を行うために必要とされる職務上の義務要件及び情報を知る必要性に基づいて行われます。アクセス権の付与又は変更については、Google 内部のデータアクセス ポリシー及びトレーニングに準拠していることも必要です。承認は、すべての変更履歴を継続的に監査するワークフローツールによって管理されています。システムへのアクセスは、アカウントビリティのための監査証跡を作成するために記録されます。認証のためパスワードが必要とされる場合（例：ワークステーションへのログイン）、少なくとも業界標準を満たしたパスワードポリシーが適用されます。この標準には、パスワードの使い回し禁止及びパスワードの十分な強さを含みます。

3. データ

(a) データの保存、隔離及び認証

Google は、Google が所有するサーバーのマルチテナント環境にデータを保存します。データ、データ処理者サービス及びファイルシステム構造は、地理的に分散した複数のデータセンターに複製されます。Google は、お客様それぞれのデータを論理的に隔離します。中央認証システムは、データの均一的なセキュリティ向上のため、すべてのデータ処理者サービスで使用されます。

(b) 廃止ディスク及びディスク破棄ガイドライン

性能上の問題、エラー又はハードウェアの障害などの発生により、データを含む特定のディスクを廃棄する場合があります（以下、「廃止ディスク」といいます。）すべての廃止ディスクは、再利用又は破壊のためにGoogle の施設を離れる前に、一連のデータ破棄プロセス（以下、「データ破棄ガイドライン」といいます。）の対象となります。廃止ディスクは複数のステップを有するプロセスによって消去され、少なくとも2つの独立した検証ソフトウェアによって消去が完全に完了したことが検証されます。消去結果は、追跡のため廃止ディスクのシリアル番号によって記録されます。最後に、消去された廃止ディスクは、再利用及び再配置のために在庫に加えられます。ハードウェアの障害により、廃止ディスクのデータを消去できない場合は、廃止ディスクは破棄されるまで安全に保管されます。各施設はデータ破棄ガイドラインの遵守状況監視のため、定期的に監査されます。

(c) 匿名データ

オンライン広告データは、それ自体が「匿名」（すなわち、追加の情報をいなければ特定の個人に帰属されることができない）とみなされるオンライン識別子に通常関連付けられています。Google は、匿名データとユーザーのGoogle アカウント情報などの個人を識別可能なユーザー情報（すなわち、それ自体が直接個人を特定し、連絡をとり、又は正確に所在を把握するために利用可能な情報）の分離を確保するために、強固なポリシー並びに技術面及び組織面のコントロールを設定しています。Google のポリシーでは、厳しく制限された状況に限って、匿名データと個人を識別可能なデータとの間の情報フローが認められています。

(d) 発売レビュー

Google は、新たなプロダクト及びフィーチャーについて、発売前に発売レビューを実施します。これには、特別に訓練を受けたプライバシー エンジニアによるプライバシーに関連するレビューが含まれます。プライバシー レビューにおいて、プライバシー エンジニアは、匿名化並びにデータの保持及び削除に関連するポリシーを限定なく含むすべての適用あるGoogle ポリシー及びガイドラインが遵守されていることを確認します。

4. 人的セキュリティ

Google の従業員は、機密保持、ビジネス倫理、適切な製品やサービスの利用及びプロフェッショナルな基準に関するGoogle のガイドラインに従って行動することが要求されます。Google は、合法的な範囲かつ適用される現地の労働法及び法定された規則の範囲内で、合理的かつ適切な経歴調査を行います。

従業員は機密保持契約を締結する必要があります。また、Google の機密保持及びプライバシーに関するポリシーの受領を確認しかつこれを遵守しなければなりません。従業員に対してはセキュリティ研修が提供されます。お客様の個人データを取り扱う従業員は、その職務に対して適切な追加的な要件も満たす必要があります。Google の従業員は、権限なくお客様の個人データを処理いたしません。

5. 処理委託先に関するセキュリティ

処理を委託するに先立って、Google は、処理委託先のセキュリティとプライバシー保護の実施状況に関する監査を行います。これは、データへのアクセス及び提供するサービスの範囲に適用レベルのセキュリティ及びプライバシー保護を処理委託先が行っていることを確認するためのものです。Google が処理委託先から提出されたリスクを評価したのち、11.3条（処理委託先への委託についての要件）に記載される要件にしたがい、処理委託先は適切なセキュリティ、機密保持及びプライバシーに関する契約条項を締結する必要があります。



## 別紙3 欧州以外のデータ保護法に関する追加規約

以下の欧州以外のデータ保護法に関する追加規約により、本データ処理規約は補足されます。

- CCPAサービス提供者付加条項 (CCPA Service Provider Addendum) ([business.safety.google/adsprocessorterms/ccpa/](https://business.safety.google/adsprocessorterms/ccpa/) に掲載) (2020年1月1日付)
- LGPD処理者付加条項 ([business.safety.google/adsprocessorterms/lgpd/](https://business.safety.google/adsprocessorterms/lgpd/) に掲載) (2020年8月16日付)
- 米国のプライバシーに関する州法のサービス提供者および処理者付加条項 (U.S. State Privacy Laws Service Provider and Processor Addendum) ([business.safety.google/adsprocessorterms/usaprivacy/](https://business.safety.google/adsprocessorterms/usaprivacy/) に掲載) (現存する CCPA サービス提供者付加条項 (CCPA Service Provider Addendum) に代わり、2023年1月1日付で有効)

Google広告データ処理規約 バージョン4.0

2022年9月21日

### 過去のバージョン

- [2021年9月27日](#)
- [2020年8月16日](#)
- [2020年8月12日](#)
- [2020年1月1日](#)
- [2019年10月31日](#)
- [2017年10月12日](#)

本規約の日本語訳は参考訳です。日本語訳と英語との間に齟齬が生じた場合、英語の原文が優先します。