



個人データ保護およびプライバシーに関する SAPのグローバルポリシー

Ver. 1.0
2012年9月



ポリシーに関するこの添付文書は情報提供のみを目的としています。これは、SAPまたはSAPの事業方向を拘束するものではありません。
また、SAPは事前の通知なくいつでもポリシーを変更する権利を有します。

目次

1.	はじめに	4
2.	データ保護およびプライバシーに関する基本原則	5
3.	データ保護およびプライバシーに関する責任	5
A.	経営幹部	5
B.	グローバル人事管理部門	6
C.	従業員	6
4.	詳細	6
A.	通知、データ精度、データへのアクセス	6
B.	データの保管期限およびデータ削除	6
C.	機密性の高い個人データに関する追加規則	7
D.	転送データおよび契約データの処理	7
5.	お客様のデータの転送	8
6.	データ保護およびプライバシーに関する監督当局	8
7.	データ保護およびプライバシーとセキュリティ	8
8.	データ保護組織	8
A.	グローバル組織	8
B.	ローカル組織、リージョン組織、および業務関連の組織	9
9.	データ保護およびプライバシーに関する基準	10
10.	認識の向上	10
付録 1:	定義	11

Page intentional blank

1. はじめに

SAP は、データ保護とプライバシー保護に取り組んでいます。SAP では、データ保護とプライバシーの権利を尊重し、SAP の責任の下にある個人情報の所有者である従業員、採用応募者、お客様、サプライヤー様、パートナー様、およびその他すべての個人のあらゆる個人データの保護に配慮しています。そのコミットメントを示すために、SAP は、この「個人データ保護およびプライバシーに関するグローバルポリシー」(以降「ポリシー」)の導入を決定しました。

本ポリシーは、個人データに関するすべての処理について要件を定義し、明確な責任と組織構造を定めることにより、SAP の法的責任下にある個人データについて、収集、処理、記録、保管、転送、開示、削除をはじめとするあらゆる処理または使用における基本的な原則を確立するものです。

SAP 内で使用する個人データの基本的な定義は、以下のとおりです(そのほかの関連の定義については付録 1 を参照してください)。

個人データとは、識別された個人または識別可能な個人に関するあらゆる情報を指します。これには、従業員、採用応募者、元従業員、お客様、見込み客、サプライヤー様、パートナー様、SAP Web サイト/サービスのユーザー、またはその他すべての個人に関するデータが含まれます。

個人とは、名前、電話番号、電子メールアドレス、住所、ユーザー ID、納税者番号、社会保障番号などにより直接的に識別される個人、あるいは何らかの情報の組み合わせにより間接的に識別される個人をいいます。個人データは、SAP が所有するシステムまたは委託システムに保管されますが、SAP 担当者がサービス、サポート、またはコンサルティング活動においてアクセスする可能性がある場合は、お客様向けとして SAP が実行しているオンデマンドシステム内、あるいはお客様のシステムまたはパートナーのシステム内に**保管される**こともあります。

SAP における個人データの収集、処理、および/または使用を伴う業務はすべて、本ポリシーで定められた規制に従うものとします。個人データの収集、処理、および/または使用を伴うプロセスすべての設計における本ポリシーの規制遵守については、経営幹部およびプロセス責任者が責任を負います。SAP の業務において個人データを扱う際に本ポリシーの規制に従うことは、SAP の従業員すべてが担う責任の範囲に含まれます。本ポリシーは、SAP の代理として SAP の個人データを処理するすべての関係者に対しても適用されます。

SAP は、ドイツに拠点を置くグローバル企業です。ドイツは欧州連合 (EU) に加盟しているため、本ポリシーは欧州データ保護法の定義に基づいていますが、本ポリシーの定める基本原則はすべての SAP 法人に適用されます。現地法(各国固有の法律)または適用されるその他の法令においてより厳格な基準が求められている場合、個人データの処理は、より基準の厳しい法律に従って行うものとします。本ポリシーの下で発行される追加の基準やガイドラインはすべて、必要に応じて、現地法または適用されるその他の法令により補完される可能性があります。適用される法令で定められた保護レベルが本ポリシーよりも低い場合、個人データの収集、処理、および/または使用に関する原則は、法律で定められたより低い保護レベルではなく、本ポリシーに基づくものとします。適用される法令についてご質問がある場合は、データ保護およびプライバシー・オフィス (DPPO) にお問い合わせください(電子メール: privacy@sap.com)。

従業員のデータ保護およびプライバシーの権利については、該当の従業員データを処理または使用する実際の場所やその国の法律ではなく、従業員契約が交わされた国の法律に従います。従業員の個人データに関する法的責任は常に、その従業員を雇用している法人組織にあります。データ保護とプライバシーについて異なる規則が従業員に適用される場合、従業員を雇用する法人は、ほかの SAP 法人に通知する責任があります(マネージャーが別の SAP 法人の従業員である場合など)。

本ポリシーは、SAP が訴訟において権利を行使する能力を制限するものではありません。

2. データ保護およびプライバシーに関する基本原則

個人データについては、その収集、処理、および/または使用を伴う業務すべてにおいて、公正に、かつ、適用される法令が認める範囲内でのみ処理されるものとします。

通常、以下の条件下での処理については認められています。

- データ主体の自由意思による同意 (Web サイトでの登録など) に基づいている、または
- データ主体との契約 (雇用契約、サービス契約など) を満たすために必要な範囲内である、または
- 法令 (税法、社会規範など) により処理が求められている、または許可されている

個人データの収集は、正当な目的がある場合のみ許可されます。その目的は、収集を実行する前に特定されるものとします。データに対する追加処理についても、別段の許可がない限り、適用される法令の条件に従うものとし、最初に指定された目的に適合しない方法で処理を行うことはできません。

個人データは、データ主体から直接収集するものとします。それが不可能な場合や当てはまらない場合は、少なくとも、該当する個人データの種類と個人データを収集、処理、および/または使用する目的についての情報をデータ主体に提示します。

収集可能なデータは、指定された目的を達成するために合理的に必要な量のデータのみとし、必要以上のデータ収集は認められません。

個人データに関しては、常に正確性が求められるため、適宜修正されます。

個人データの保管は、指定された目的のために必要な期間に限り認められるものとします。

3. データ保護およびプライバシーに関する責任

a. 経営幹部

SAP における個人データの収集、処理、および/または使用が、適用される法令に従って行われるようにする法的責任は、それぞれの業務上の目的で該当個人データを収集、処理、および/または使用する各 SAP 法人の経営幹部 (SAP AG の役員、社長など) にあります。

SAP 内部では、責任および説明責任の委譲についての明示的な指定を含む文書化された管理上の指示、指図、ビジネスプロセスの定義を介して、SAP の組織構造に沿ってさまざまなレベルのマネージャーや従業員に責任が委譲されます。

経営幹部は、個人データの収集、処理、および/または使用に関するすべてのプロセスの設計が、本ポリシーの要件を満たすものとなるようにする責任を負います。

各 SAP 法人の経営幹部は、以下の点についての責任を負います。

- 各地域のデータ保護およびプライバシー担当コーディネーターの任命などによる、現地法 (各国固有の法律) の監視 (セクション 8b を参照)
- グローバルプロセスが現地法に準拠していることの確認と、現地の法令が該当のプロセスに影響を及ぼす場合に、ローカルおよびグローバルプロセス責任者に関連情報が提供されていることの確認
- 現地法において、個人データの収集、処理、使用、または転送に関する監督当局への通知または (事前) 承認が求められている場合の、関連当局との連絡

b. グローバル人事管理部門

SAP または SAP のビジネスパートナーのいずれの管理下にあっても、個人データへのアクセス権を持つ従業員には、適用される法令に基づく個人的な責任についての情報が適宜提供され、個人としてデータに関する守秘義務が課せられます。この義務については、書面または検証可能な形で証明するものとします。守秘義務は、適用される法令に従って、SAP の代理として行動する従業員および個人すべてに課せられます。従業員に課せられる義務には、適用されるデータ保護およびプライバシー関連の法令に対して何らかの違反があった場合の個人責任および法的責任も含まれます。

SAP が管理する個人データへのアクセス権を持つ SAP 従業員および第三者による守秘義務の履行についての責任は、SAP のグローバル人事管理組織にあります。

c. 従業員

すべての SAP 従業員は、SAP におけるそれぞれの職務のためにアクセス権を保有している個人データについて、守秘義務を遵守する責任があります。

SAP の従業員に対しては、承認されたプロセスに従って、それぞれの職務を果たすために必要な範囲内に限り、個人データの収集、処理、および/または使用が許可されます。ただし従業員は、個人データの使用に関する管理上の指示の合法性については責任を問われないものとします。疑念がある場合、従業員は経営幹部またはデータ保護およびプライバシー・オフィス (privacy@sap.com) を通じて説明を求めることができます。従業員は、それぞれの義務(データに関する守秘義務など)の履行については、個人として説明責任を負います。

4. 詳細

a. 通知、データ精度、データへのアクセス

すべてのデータ主体に対し、通常はデータ収集に先立って、適用される法令に従い、個人データの収集、処理、および/または使用に関する適切な情報を提供するものとします。

データ処理活動に関するデータ主体への通知は、誤解を招く情報や表現を避け、簡潔かつ分かりやすい方法で行わなくてはなりません。

保存された個人データについては正確性を維持する必要があるため、不正確な個人データについては修正または削除するための適正な措置を講じます。

データ主体は、いつでも各自の個人データへのアクセスを要求することができます。個人データの収集、処理、および/または使用を伴うすべてのプロセスには、修正および更新の可能性があるものとします。また、適用される法令によって求められる場合は、必要に応じて削除またはブロックされる可能性もあります。データ主体からの要求またはクレームについては、担当の SAP 法人が適時に処理を行います。データ主体から、それぞれの個人データの処理に関して異議の申し立てがあった場合は、適法に検証を行い、必要に応じて修正措置を講じるものとします。

従業員は、データが保存されている場所または処理される場所にかかわらず、雇用されている国の法律に従って個人データにアクセスできる必要があります。不正確または不完全な個人データがある場合、従業員はデータの修正、または必要に応じてブロックもしくは消去を求めることができます。

すべてのデータ主体は、SAP 法人または SAP の代理として処理を行う外部ベンダーによって保存または処理される各自の個人データの性質について照会する権利を有します。

b. データの保管期限およびデータ削除

個人データの収集、処理、および/または使用を伴うあらゆる処理に関しては、特定の目的が達成された後、あるいは法的根拠に基づく期間を経過した後に、該当個人データが削除、匿名化、またはブロックされるようにするためのスケジュールを明示するものとします。すべての処理において、このような定期的な削除が求められます。

個人データについては、削除する代わりに永続的に匿名化される、すなわち個人の識別ができない形で保存される可能性があります。技術的または法的な理由のために削除と匿名化がいずれも不可能な場合（法律によって課税目的で記録を保管することが求められている場合など）は、該当の個人データをそれ以上処理および/または使用できないようにし、その個人データへのアクセスを正当な必要性がある個人のみを制限します。

c. 機微個人データに関する追加規則

機微個人データとは、個人情報を含む特別なカテゴリーの個人データのことです。具体的には、各個人の医学的状態または健康状態、人種または種族的出身、政治的見解、宗教的または哲学的信条、刑事上の有罪判決、労働組合への加入状況、または個人の性的指向に関する情報などを示すデータを指します。

SAP または SAP の代理としての第三者が機微個人データを収集する必要がある状況においては、その機微データを取得する理由とそれを共有する関係者についての情報がデータ主体に確実に提供されるように、経営幹部が必要な措置を講じます。これらの機微個人データの処理および転送については、適用される法律に従って、データ主体からの明示的な同意を得るものとします。また、データの性質および使用目的に伴うリスクに応じて、適切な保護手段（物理的なセキュリティデバイス、暗号化、アクセス制限など）を提供します。

こうした特別なカテゴリーのデータに対しては、以下の追加規則が適用されます。

- 該当データの収集、処理、および/または使用に関しては、各データ主体に対して常に透明性を提供する
- 個別のデータ主体から同意を得る場合は常に、該当データを明示する
- 機微個人データの収集または使用を伴うプロセスは、データ保護およびプライバシー・オフィスまたは各地域のデータ保護およびプライバシー担当コーディネーターの事前承認を得た場合のみ作成できる

d. 転送データおよび契約データの処理

今日のビジネス界では、1 つの会社の複数の関連会社間、あるいはほかの会社との間で個人データがやり取りされることは珍しいことではありません。このような個人データのやり取りが行われるのは、1 つの会社または関連会社が別の事業体の代理としてデータを処理する場合（「処理のための転送」）や、データを受け取る事業体が独自の目的で個人データを使用する場合（「独自の目的のための転送」）です。いずれの状況においても、セキュリティとデータ保護に関する契約条項が必要です。

また、欧州連合 (EU) 域内の SAP 法人の法的責任下にある個人データについての、欧州経済地域 (欧州連合に、ノルウェー、アイスランド、およびリヒテンシュタイン公国を合わせた地域) 外での処理、あるいはこの地域外への転送は、EU のデータ保護指令 95/46/EC の 25 条および 26 条に従って、適切な法的保護措置が講じられている場合のみ行われるものとします。

個人データを転送する場合は、以下の規則が適用されます。

SAP の代理として処理を行うための転送:

SAP は、データ主体に対する義務に関して、常に法的責任を果たします。第三者であるサービスプロバイダーにデータを引き渡した場合や、そのサービスプロバイダーがデータを使用する場合も、これらの義務が解消されることはありません。

SAP が、サービスプロバイダーに対し、SAP に代わって個人データの処理を含むタスクを行うことを委託する場合は、セキュリティおよびデータ保護に関する契約条項が必要となります。そのため、契約上のデータ処理に関与するサプライヤーをチェックするプロセスを導入し、維持管理に努めることとします。また、サプライヤーに対して SAP の法律上および契約上の義務と要件の遵守に関する事前確認を行うことなく、契約上データ処理を含むサービスを委託することはありません。

データを受け取る会社独自の目的のための転送:

第三者に対してその第三者が使用するために個人データを転送すること、あるいは国家または国際機関に個人データを転送することは、法律で許可または必要とされている場合か、該当するデータ主体から事前の同意を得ている場合のみ可能とします。

SAP 法人間での転送

SAP は、SAP 法人間での個人データの転送に関する合法性を確実なものとするため、すべての SAP 子会社および SAP 法人と、「会社間マスターデータ保護契約」を締結しています。法人の合併、分割、および買収が行われる場合も、そのすべてが契約の履行を通じてこの枠組みに組み込まれます。法人間で転送された個人データの使用については、マスターデータ保護契約で定められた規則に従うものとします。また、適用されるデータ保護法律を確実に遵守するために何らかの枠組みが導入された場合は、その枠組みの規則にも従うものとします。ここでいう適用されるデータ保護法律とは、特に EU のデータ保護指令および関連の現地法を指しますが、必ずしもこれらに限定されるものではありません。

買収、分割、または新会社設立の場合、新規に買収した法人または設立された法人が「会社間マスターデータ保護契約」に完全に合意しない限り、その法人に対して個人データの転送や個人データへのアクセス権限が許可されることはありません。

5. お客様のデータの転送

SAP では、お客様の個人データの処理を、お客様の代理として行っています。こうしたお客様データを転送および使用する場合は必ず、適用される法令と契約で定められた義務に従って行うものとします。お客様の個人データが、法律または契約に基づく適切な根拠なく第三者に転送されることは決してありません。

この点に関しては、SAP では、お客様と連携を図り、お客様の側でも適用されるデータ保護法を遵守できるように支援を行っています。

6. データ保護およびプライバシーに関する監督当局

SAP 法人は常に、現地法、契約上の義務、または本ポリシーの求めに応じて、データ保護に関する監督当局に協力します。また、こうした協力については、国を越えて行うものとします。

データ保護およびプライバシーに関する監督当局が何らかの情報を求めている場合や監督権を行使する場合は、ローカルの法務組織とデータ保護およびプライバシー組織に迅速に通知するものとします。国を越えた活動については、SAP のデータ保護およびプライバシー・オフィスと連携するものとします。

7. データ保護およびプライバシーとセキュリティ

データ保護およびプライバシーに関する法令においては、特定のセキュリティ対策が求められています。SAP では、こうした対策について、SAP セキュリティポリシーとそれに付随するセキュリティ標準およびガイドラインで定義しています。これらの標準およびガイドラインの定義および更新については、データ保護およびプライバシー・オフィスがサポートを提供します。

8. データ保護組織

a. グローバル組織

データ保護およびプライバシー・オフィスは、担当役員直属の、SAP AG 内部の組織単位です。

データ保護およびプライバシーに関するグローバルレベルでのガバナンスについては、SAP データ保護オフィサーが率いるデータ保護およびプライバシー・オフィスが担当します。SAP データ保護オフィサーの独立性は、ドイツ連邦データ保護法 4f 条の規定に従って保証されています。

グローバル組織が担当するタスクの定義については、付録 2 に記載されています。

b. ローカル組織、リージョン組織、および業務関連の組織

ローカル、リージョン、業務部門 (LoB) の管理については、ローカル組織やリージョン組織、または LoB 固有の組織を設立し、特に以下の措置を講じるものとします。

- データ保護およびプライバシーに関するグローバルネットワークの一部として、データ保護およびプライバシー担当コーディネーターを任命します。
データ保護およびプライバシー担当コーディネーターは、複数の国を対象として任命されることも 1 つの地域全体に対して任命されることもあります。いずれの場合も国ごとの責任については常に明確にするものとします。また、各法人の社長、あるいはリージョンや LoB のマネジメントの統括責任者 への直接的または機能的な報告システムを確立します。
- データ保護およびプライバシー担当コーディネーターに対し、職務を遂行するための適切なリソースを提供します。
- データ保護およびプライバシー担当コーディネーターおよび DPPO が、関連のプロジェクトに適時に関与できる体制を整えます。

SAP では、すべての法人において、データ保護およびプライバシー担当コーディネーターを配置しなくてはならないものとします。

DPPO においては、データ保護およびプライバシーに関する国ごとのガバナンス体制が十分ではありません。そのため、国またはリージョンレベルでデータ保護およびプライバシー担当コーディネーターが配置されているかどうかにかかわらず、以下の業務部門においてはデータ保護およびプライバシー担当コーディネーターを任命する必要があるものとします。

グローバルレベル:

- グローバル人事管理
- グローバルサービスおよびサポート
- クラウドビジネスユニット
- エコシステムおよびチャネル
- SAP グローバルマーケティング
- グローバル IT
- SAP Research
- グローバル財務および管理
- 開発

リージョンレベル:

- コンサルティングサービス

ローカル組織、リージョン組織、または LoB 関連の組織が担当するタスクの定義については、付録 3 に記載されています。

9. データ保護およびプライバシーに関する基準

本ポリシーは、個人データを一般的な方法で処理する際の SAP、SAP マネージャー、および SAP 従業員の義務および職務について示すものであるため、固有の方法でガイドライン、手順、作業指示を作成して業務で使用可能な文書を提供する場合は、ローカルのまたはトピック固有のニーズが生じます。

そのため、DPPO またはローカル、リージョンまたは LoB のデータ保護およびプライバシー担当コーディネーターらが、場合によっては密接に連携して、データ保護およびプライバシーに関する基準を策定、導入、および更新するものとなります。これらの基準については、DPPO が検討を行って承認します。また、リージョンレベルまたはグローバルレベルの基準については、データ保護およびプライバシー運営委員会による承認が必要です。

これらの基準は、本ポリシーで定める義務と矛盾するものであってはいませんが、本ポリシーの一般的なステートメントを拡大適用したり明定したりすることは可能とします。

10. 認識の向上

DPPO およびデータ保護およびプライバシー担当コーディネーターは、認識を高めるためのプログラムを定期的に作成するものとしてします。また、従業員および SAP のために働く個人すべてに対し、それぞれの義務と職務に関する情報に加え、本ポリシーおよび適用される法令により保護される権利についての情報を定期的に提供します。

付録 1:

定義

匿名データ	ほかのデータまたは情報により間接的に識別される場合を含め、いかなる形でも個人の識別が可能でない形式でのデータ。ただし匿名データについては、データ保護およびプライバシーに関する内部または外部の規制対象には含まれません。
収集、処理、および/または使用	「収集」とは、データ主体に関するデータの取得を意味します。「処理」は、個人データに対して実行されるすべての操作または一連の操作(自動的な手段による操作もそれ以外の操作も含む)のことで、これには個人データの収集、記録、調整、保存、変更、転送、ブロック、消去などが含まれます。「使用」は、処理以外の個人データの利用すべてを指します。
同意	明示的な同意と暗黙的な同意があります。一般的に、明示的な同意を得るには、データに対する何らかの処理をデータ主体が許可する行動(電子メールの送信や個人データの収集に対するオプトインなど)が必要となります。自由意思に基づいて表明された明示的な同意は、別途法律による規制がない限り、個人データを処理する正当な根拠とみなされます。暗黙的な同意(オプトアウトなど)の場合は、データ主体が別段の意思表示を行わない限り、処理が許可されます。
管理者	単独あるいは他者と共同で、個人データの処理に関する目的と手段を決定する個人または法人(一般的な法的定義)。SAP においては、常に SAP 法人が、従業員、顧客サプライヤー、パートナーその他の個人に関する個人データの管理者となります。SAP 従業員、SAP 内部ユニット、または SAP 社内組織が管理者となることはありません。管理者となるのは、SAP AG の役員やほかの SAP 法人の社長など、法的な責任を有する経営幹部です。
データ主体	識別された個人、または識別可能な自然人。識別可能な個人とは、特に ID 番号、または 1 つまたは複数の身体的、生理的、精神的、経済的、文化的、または社会的な識別性を示す固有の要素を参照することにより、直接的または間接的に識別できる個人を指します。
削除	データの物理的な破壊、またはデータと自然人との関係をそれ以上識別できない方法でのデータの匿名化。
個人データ	識別された個人または識別可能な自然人(データ主体)に関するあらゆる情報。識別可能な個人とは、特に ID 番号、または 1 つまたは複数の身体的、生理的、精神的、経済的、文化的、または社会的な識別性を示す固有の要素を参照することにより、直接的または間接的に識別できる個人を指します。

処理担当者	管理者の代理として個人データを処理する自然人、法人、公的機関、代理店、またはその他の組織(外部法人、管理者の所属先とは別の SAP 法人など)。
特別なカテゴリーの個人データ	人種または種族的出身、政治的見解、宗教的または哲学的信条、労働組合への加入状況、犯罪歴、刑事上の有罪判決、健康状態、性生活に関するデータ、および個人情報の盗難に使用される可能性のあるデータ(社会保障番号、クレジットカード番号、銀行口座番号、パスポート番号、運転免許証番号など)が含まれます。
第三者	管理者または処理担当者の直接的な管轄下でデータを処理することを認められた、データ主体、管理者、および処理担当者以外の自然人、法人、公的機関、代理店、またはその他すべての組織。SAP グループ内の異なる法人は、相互に第三者とみなされます。

付録 2 および付録 3 は、SAP 社内用です。一般公開されているこのバージョンには含まれていません。

© 2013 SAP AG. All rights reserved.

SAP、R/3、SAP NetWeaver、Duet、PartnerEdge、ByDesign、SAP Business Objects Explorer、StreamWork、SAP HANA、および本書に記載されたその他の SAP 製品、サービス、ならびにそれぞれのロゴは、ドイツおよびその他の国々における SAP AG の商標または登録商標です。

Business Objects および Business Objects ロゴ、Business Objects、Crystal Reports、Crystal Decisions、Web Intelligence、Xcelsius、および本書で引用されているその他の Business Objects 製品およびサービス、ならびにそれぞれのロゴも含めて、Business Objects Software Ltd の商標または登録商標です。Business Objects は SAP の子会社です。

Sybase および Adaptive Server、iAnywhere、Sybase 365、SQLAnywhere、および本書で引用されているその他の Sybase 製品およびサービス、ならびにそれぞれのロゴも含めて、Sybase Inc の商標または登録商標です。Sybase は SAP の子会社です。

Crossgate、m@gic EDDY、B2B 360°、および B2B 360° Services は、ドイツおよびその他の国々における Crossgate AG の登録商標です。rossgate は SAP の子会社です。

本書に記載されたその他すべての製品およびサービス名は、それぞれの企業の商標です。本文書に含まれるデータは、情報目的でのみ提供されます。製品仕様は、国ごとに変わる場合があります。

これらの文書の内容は、予告なしに変更されることがあります。これらの文書は SAP AG およびその関連会社（「SAP グループ」）が情報提供のためにのみ提供するもので、いかなる種類の表明および保証を伴うものではなく、SAP グループは文書に関する誤記・脱落等の過失に対する責任を負うものではありません。SAP グループの製品およびサービスに対する唯一の保証は、当該製品およびサービスに伴う明示的保証がある場合に、これに規定されたものに限られます。本書のいかなる記述も、追加の保証となるものではありません。