elastic

Elasticを活用して世界のプライバシー法の遵守を推進

エグゼクティブサマリー

現代のデジタル世界で事業運営を成功させるために、組織はデータ、特にAIにおけるその役割に注目しています。これに対応して、プライバシー法や規制の爆発的な増加が世界のビジネス環境を再構築しています。これらの規制の進展に対応することは、単なるリスクの軽減や緩和にとどまらず、重要で強力な市場差別化要因となります。急速に変化する法的および規制上のプライバシー環境へのコンプライアンスは、顧客の信頼を高め、財務成長を促進し、運用の回復性を強化する可能性もあります。

このホワイトペーパーでは、データプライバシー法の重要な概念を紹介し、組織がElasticの強力なプラットフォームをデプロイし、適用される個人データ要件を満たすだけでなく、迅速かつ効率的にこれらを運用化する方法を示します。世界中のデータプライバシー規制に広く適用される6つの基本的なプライバシー原則を概説し、これをElasticのプラットフォームソリューションにマッピングして、組織がデータプライバシーをコンプライアンス義務から競争上の優位性へと変えられるよう支援します。

注意：このホワイトペーパーは情報提供のみを目的としており、法的助言を構成するものではありません。法的助言については、ご自身の法律顧問にご相談ください。

 © 2026 Elasticsearch B.V. All rights reserved.

背景と世界のプライバシー法入門

世界的なプライバシー法は、個人データを収集する組織にとってますます複雑な課題を生み出しています。個人データが世界で最も価値のある商品の1つと広く見なされている中、プライバシー法の遵守は企業にとって重要なビジネス推進力となり得ます。そして、遵守に失敗すると、企業の成長を著しく妨げる可能性があります。

組織が収集する個人データが増えるにつれて、そのデータを管理・保護するためのスケーラブルなソリューションを見つけることが、プライバシーを重視する世界において説明責任を果たし、信頼できるベンダーとしての評判を築く上でますます重要になります。

さまざまなプライバシー法には違いがありますが、その多くは特定の包括的な原則を共有しています。

主なプライバシー法には以下が含まれます。

- EUの一般データ保護規則（「GDPR」）および英国の類似規則
- カリフォルニア州消費者プライバシー法（「CCPA」）のような米国の州のプライバシー法
- ブラジル一般データ保護法（「LGPD」）
- カナダの個人情報保護および電子文書法（「PIPEDA」）
- 日本の個人情報保護法（「APPI」）

Elasticのプラットフォームが提供する柔軟性とスケールにより、組織はこれらの多様で複雑な法的要件へのコンプライアンスに対応し、管理することができます。

 © 2026 Elasticsearch B.V. All rights reserved.

個人データ

「個人データ」の概念が、氏名、メールアドレス、政府発行の識別子、電話番号などの明白な識別子に限定されていた時代は過ぎ去りました。現在、世界のプライバシー法は、特定のデバイスや個人に関連するあらゆる情報を捉えるために広義に個人データを定義しています。

経験則としては、個人の一意の識別子に結び付けられる情報に関しては、プライバシー法が適用される可能性が高いと想定するのがよいでしょう。スマートフォン、IoTデバイス、その他のコンピューティングデバイスが日常生活に遍在する中、あらゆる業界の組織において個人データの収集が急増しており、そのようなデータの処理を自信を持って管理できる製品とサービスに対する喫緊かつ否定できないニーズが生じています。

管理者と処理者

世界中のプライバシー法では、通常、組織が個人データの「管理者」として機能するか「処理者」として機能するかに応じて、組織に異なる（ただし多くの場合は重複する）義務を課しています。

- **管理者**（CCPAでは「事業者」とも呼ばれます）は、個人データの処理目的と手段を管理します。管理者は、どのような個人データを収集し、どのように処理するかについて、独立した決定権を持つ主体です。
- **処理者**（CCPAでは「サービスプロバイダー」とも呼ばれます）は、上流の管理者（または場合によっては別の処理者）にサービスを提供し、管理者へのサービス提供のために、管理者の指示に厳密に従って個人データを処理することのみが許可されています。

管理者と処理者には異なる義務が適用されますが、それぞれの役割におけるコンプライアンスには、処理される個人データの種類を理解し、ターゲットを絞ったスケーラブルで効率的な方法で個人データを見つける能力が必要となります。

世界中のほとんどのプライバシー法では、個人がデータへのアクセス、削除、修正など、特定の権利を行使することも認められています。比較的短期間で対応する必要がある場合、Elasticのようなプラットフォームを使用して非構造化および構造化データセットを効率的に精査することで、コンプライアンスを合理化するだけでなく、規制調査や民事訴訟のリスクを軽減することができます。

 © 2026 Elasticsearch B.V. All rights reserved.

プライバシーの基本原則

世界的なプライバシー法は、多くの場合、基礎的なプライバシー原則に基づいています。大まかには次のようになります。

1

通知

プライバシー法では、組織がプライバシー慣行について正確かつ最新の通知を提供することを義務付けています。

2

プライバシー・バイ・デザイン

プライバシー法では、組織は自社の慣行がプライバシー権や個人の利益にどのような影響を与えるかを十分に検討し、それらの法律に準拠するように製品を設計することが義務付けられています。

3

権利

プライバシー法により、個人は個人データに関して一定の権利を有します。これには、データへのアクセス、削除、および修正の権利が含まれる場合があります。

4

データの最小化

プライバシー法は、組織に対してデータの最小化（つまり、収集された個人データのビジネス目的に必要な個人データのみを収集および処理すること）を実践し、組織が必要としないデータを保持しないようにするために保持制限と削除ポリシーを課すことを要求しています。

5

セキュリティ

プライバシー法は、個人データを保護するために特定のセキュリティ基準を義務付けています。

6

違反通知

プライバシーおよびセキュリティ法は、個人データに影響を与えるセキュリティインシデントやデータ侵害が発生した組織に対して、多くの義務を課しています。

 © 2026 Elasticsearch B.V. All rights reserved.

不遵守のコスト

プライバシー法に違反すると、高額の罰金、訴訟費用、評判の失墜につながる可能性があります。GDPRやCCPAのようなフレームワークの下での規制上の罰則は、企業の収益に重大な影響を与えるほど厳しいものになることがあります。一方、民事訴訟当事者が、データ侵害後の集団訴訟など、プライバシー侵害の申し立てを行うこともあります。

IBM SecurityとPonemon Instituteのレポートによると、2024年のデータ侵害の平均コストは488万ドルで、前年比10%の増加となりました。AONのサイバーリスクレポートによると、2024年に大々的に報道された56件のサイバーインシデントにより、影響を受けた組織の株価は平均27%下落しています。こうした風評被害が組織の競争優位性に取り返しのつかない影響を与えることは明らかです。このような状況を踏まえると、コンプライアンスは単なるコストではなく、戦略的投資です。

 © 2026 Elasticsearch B.V. All rights reserved.

データ保護コンプライアンスのニーズにElasticを活用

Elasticは、オープンで柔軟なエンタープライズソリューションにより、組織が重要な関連回答をかつてないほど迅速に見つけられるよう支援します。世界のプライバシー法を遵守するには、個人データがどこにあるか、どのように移動するか、そしてそのデータがどのように処理されるかについて、データエコシステム全体を理解する必要があります。ここでElasticsearch Platformが活躍します。これらのプロセスを簡素化・自動化し、シームレスなコンプライアンスを実現します。以下では、上で説明した6つの基本的なプライバシー原則と照らし合わせたElasticの価値について概説します。

通知

Elasticのデータマッピング機能により、組織は組織のサーバーやそれ以外の場所にある個人データの範囲と種類を把握できます。

通知はプライバシー法の中核となる基本原則です。個人は、組織が自分に関して収集する個人データの種類、収集目的、そしてデータが他の当事者に開示される状況を理解する権利を有します。データプライバシー法では、組織にElasticのプライバシーステートメントのような包括的なプライバシーポリシーを提供し、これらの概念を説明（Elastic Trust Centerで示されているように）することが求められることがよくあります。

この通知原則に従うには、組織は収集する個人データの範囲を理解する必要があります。これには、組織内のすべての個人データフローを識別して文書化する体系的なプロセスである堅牢なデータマッピング作業が必要です。

スケーラブルなソリューションがなければ、組織は収集された個人データとそのデータが組織内外でどのように移動するかを特定するために、雑多な旧式のスプレッドシート、データインベントリ調査への回答、さまざまな事業部門との場当たり的なインタビューに頼らざるを得なくなることがよくあります。

 © 2026 Elasticsearch B.V. All rights reserved.

運がよければ一時的に正確な記録が見つかる可能性はありますが、データに支えられた経済においては、データ収集と処理の要求に悩まされることになります。

Elasticは、組織がデータマッピングプロセスを改善するための重要な洞察を得るのに役立ちます。収集される個人データの種類、そのデータの保存場所と開示先を把握しなければ、組織はプライバシー法の遵守を確認できません。Elasticに流入するデータに関する情報をインデキシングすることで、強力な全文検索機能により、個人データに依存するアプリケーション、テーブル、クエリ、レポートを迅速に識別できるようになります。

Elasticを使用してデータマッピングを合理化することで、組織がプライバシー法の契約義務を遵守するのにも役立ちます。識別されたデータフローによって、組織がデータ保護補遺、データ転送メカニズムや個人データの保護に特化したその他の契約を締結すべき他の当事者が決まるためです。同様に、今日のサプライチェーンは、数百または数千のベンダーやサブプロセッサーに及ぶ可能性があります。何千もの契約書を瞬時にインデックスし、全文検索を実行できる機能により、ベンダーのステータスレポートも容易になり、さらに重要な点として、プロアクティブなベンダー管理プログラムが可能になります。

プライバシー・バイ・デザイン

組織はElasticを使用して、データ最小化の原則を組み込むなど、設計段階からプライバシーを強化できます。

個人データのデータストアとしてElasticの利用を検討されている場合、Elasticの中心的なオーケストレーションソフトウェアであるElastic Cloud Enterprise（以下「ECE」）の機能を利用することで、組織は最初から適切な軌道に乗ることができます。設計により組み込まれたデータ保護の原則とは、アクセスを制限し、正確性を維持し、適切なデータセキュリティ管理を実施し、保存期間を制限することで個人データを貴重な資産のように扱うことです。

単一の巨大なデータストアと、複雑に重複する大量のデータアクセス制御（さまざまなプロジェクトによる特定データへのアクセスのみを許可するために必要）を備えた従来のデータアーキテクチャとは異なり、Elasticなら、ユーザーはプロジェクトごとに新しいElasticsearchクラスターをインスタンス化し、そのプロジェクトに関連するデータのみをクラスターに含めることができます。

 © 2026 Elasticsearch B.V. All rights reserved.

この分散型アーキテクチャにより、プライバシーのもう1つの中核原則である個人データの最小化を実現できます。例えば、お客様はElasticを使用してデータをストレージ階層に分類できます。Elasticが提供するアクセスログ情報により、企業は未使用のデータを特定し、データ保持の方針や慣行に役立てることができます。

また、Elasticを使用すると、組織はデータプライバシー影響評価（「DPIA」）をいつ、どのように実施すべきかを理解することができます。GDPRおよび同様のプライバシー規制では、DPIAは、個人データを責任を持って処理し、個人への潜在的な損害を最小限に抑えていることを確認するために使用される、場合によっては必須の評価です。データがどこにあり、どのように処理され、どこに流れているかを知ることで、個人データの使用を理解するためにこれまで事業部門全体で多面的なサポートが必要だったDPIAを効率的に完了できます。DPIAは、基本的なコンプライアンスを実証すると同時に、組織が個人データの処理を世界的なプライバシー法で許可されている範囲に制限できるようにします。

データ主体の権利

組織はElasticを使用して関連する個人データを識別し、データ主体の権利の適用可能性を評価し、データ主体の要求を尊重できます。

世界的なプライバシー法では、個人に個人データの処理方法に関する一定の選択肢を与えています。これらには通常、個人データへのアクセス、削除、修正の権利、特定の種類の個人データの処理に異議を申し立てる権利が含まれます。Elasticのデータマッピング機能は、組織がデータ主体の要求を処理するための中核的な基盤を形成します。

- **アクセス：**Elasticsearchを使用することで、組織は、データストアを検索して、個人データに依存するテーブル、クエリ、レポート、アプリケーションを特定するなど、組織全体の個人データを特定できます。また、Elasticを活用してエンドユーザーの検索機能を強化でき、エンドユーザーはセルフサービスツールを使用してデータを識別してエクスポートできます。セルフサービスツールでは対応できない場合も、組織はElasticを使用してデータストアを迅速に検索し、データ主体のアクセスリクエストに対応することができます。

 © 2026 Elasticsearch B.V. All rights reserved.

- **削除：**Elasticを使用してある個人に関する個人データを特定した後、組織はElasticを使用してそれらのデータをさらに変換できます。これには、削除例外を適用して保持するためのデータのタグ付け、データの永久削除、匿名化や特定の種類の個人データの仮名化など、プライバシー法で許容される可能性のあるその他の削除手法の使用が含まれます。Elasticを使用すると、個人データを迅速かつコストのかかるエンジニアリング作業なしで変換できるため、組織はコンプライアンスを維持し、規制当局の調査を回避し、グローバルなプライバシー法の範囲内でデータの有用性を維持できます。
- **修正：**同様に、プライバシー法では個人が個人データの修正を要求することがしばしば認められています。Elasticは個人に関する個人データを分離できるため、組織はデータの検索ではなく、要求の処理に集中できます。
- **制限：** GDPRやその英国版のような個人情報保護法には、個人データの処理に異議を唱える権利や制限を要求する権利も含まれています。Elasticのデータマッピングやデータ分類機能を利用することで、このような要求にどのように対応すべきかを迅速に把握し、それに応じてアクセスや利用許可を制限することができます。

データの最小化

*「プライバシー・バイ・デザイン」*セクションでも触れたように、Elasticは、企業向けのデータ最小化機能を強化します。データ最小化の原則では、組織が個人データの収集、処理、保持を制限し、組織の認可された処理目的を達成するために必要な情報に限定することを義務付けています。

例えば、この義務を果たすために個人データの処理を最小限に抑える方法には**仮名化**（データ内の個人識別子をプレースホルダー値に置き換える）や**匿名化**（個人を特定できないようにデータから個人識別子を完全に削除する）があります。欧州の大手航空会社がElasticの取り込みパイプラインを使用して機密データをストレージ前に難読化する方法をご覧ください。このような成果は、Elasticで利用可能な統合であるLogstashを使用して実現できます。Logstashは多数のソースからデータを取り込み、匿名化や仮名化などのデータの変換を促進し、データ最小化の目標を前進させ、データセキュリティリスクを軽減します。

データのマッピングと監査にElasticを使用することで、組織は保持されている個人データの実際の使用状況をより詳細に分析できるため、データ保持期間とポリシーをより効果的に調整できます。

 © 2026 Elasticsearch B.V. All rights reserved.

セキュリティと侵害通知

Elasticが組織の個人データを保護し、データ侵害が発生した場合に迅速に対応する方法についての詳細は、セキュリティホワイトペーパーをご覧ください。

まとめ

データプライバシーは単なる規制上の要件ではなく、ビジネス上の必須事項です。高額な罰金、業務の中断、評判の失墜、顧客の信頼を失うリスクがあるため、組織には、データのマッピング、分類、管理、変換、分析、削除を行うための信頼性が高くスケーラブルな方法が必要です。Elasticは、このプロセスのすべてのステップを合理化し、コンプライアンスと顧客の信頼のために組織が必要とするスケーラブルなパワーを提供します。

 © 2026 Elasticsearch B.V. All rights reserved.