Informatica

ホワイトペーパー

GDPRの「D」に対処する方法の提案

インフォマティカについて

デジタルトランスフォーメーションによって我々の期待値が変化しています。より良いサービスを、素早く、便利に、低コストで利用したいという期待が高まっているのです。企業も状況に応じて変化する必要があります。そしてそのヒントは「データ」にあります。

エンタープライズ向けクラウドデータ管理で世界をリードするインフォマティカは、俊敏性の向上、新たな成長機会の獲得、新しいソリューションの開発を実現するための洞察を通じて、あらゆる産業や分野の企業がインテリジェントにビジネスをリードできるよう支援します。インフォマティカは、あらゆるデータを徹底的に重視し、企業の成功に必要とされる汎用性を提供します。

インフォマティカは、企業がこれからのインテリジェントな破壊的イノベーションを推進できるよう、当社が提供するあらゆるサービスを通じてデータの力を継続的に引き出すことを支援します。

目次

1.エグゼクティブサマリー

2018年5月より欧州連合の一般データ保護規則（GDPR）が施行され、個人情報の保護がさらに強化されます。GDPRは、EU域内に拠点を置く事業者をはじめ、EU域内の個人に商品やサービスを提供する場合やその個人の活動を監視または追跡する場合に個人情報を取り扱う全事業者（EUを含めたすべての国）に適用されます。この規制は多くの企業に大きな影響を与え、顧客や消費者、パートナーや従業員、その他の「データ主体」（個人・集団）に関するデータの管理方法を大きく変える可能性があります。個人のデータレコードのストレージや処理、アクセスや転送、公開に影響が出るだけでなく、違反した場合は多額の罰金が科せられる可能性があります。

GDPRでは、データプライバシーに関する新たな要件を盛り込み、市民のプライバシーの権利を強化しています。企業に対しては、現在および将来の情報資産の利用状況をすべて把握することを義務付けています。企業では、これに伴う情報管理態勢の変更に対応すべく、現在と将来のデータ機能を徹底して評価しなくてはなりません。このホワイトペーパーでは、このような要件を分析し、データに関する課題やGDPRに備えて進むべき方向性を明らかにする方法を説明します。

さらに理解を深めていただくため、GDPRへの取り組みにおいて多くの企業に共通する質問も取り上げています。これらをエントリーポイントの質問と呼びます。エントリーポイントの質問に対する答えを見つけやすくするため、インフォマティカが重要と考える機能と、各機能に応じたテクノロジーの使用事例（その機能をどのように開発できるか）をまとめました。各項目の関連性を下表に示します。

エントリーポイントの質問	必要な機能	テクノロジーの使用事例
対象になりうるすべてのデータはどこにあるか？	機密データディスカバリ＆リスク分析	検出と保護
個人情報をどのように使用しているか？	ポリシー解釈	企業データのガバナンス
データ主体の情報をどのように管理しているか？	個人情報管理	データ照合と関連付けの使用事例
どのようにデータを保護し、不正アクセスを防止しているか？	データセキュリティ管理の実施	検出と保護

同意の取得と管理など様々な要件が、複数の機能やテクノロジーの使用事例にまたがる場合もあります。そのため、潜在的な複雑さのレベルを明確に把握しておく必要があります。

GDPRには数々の課題が伴う一方、データの利用について多くのチャンスも生まれます。このホワイトペーパーでは、使用事例のアプローチを紹介し、データ管理におけるインフォマティカの豊富な経験に基づいてアドバイスを行っています。企業は、様々な課題を解決すると同時に、データ管理、ガバナンス、セキュリティについて革新的な機能を導入してコンプライアンスプログラムの成果を最大限に引き出すことが可能になります。インフォマティカは、データの自動化、保護、制御に役立つ革新的な統合ソフトウェアソリューションを提供しています。これらのソリューションを活用することで、GDPRへの対応を速やかに進めることができます。

2.背景

2.1 背景および予測される影響

社会のデジタル化が急速に進む中、ほぼすべての企業では、データのパワーを活かして業務上の意思決定を改善したり、顧客やパートナーとつながりを築いたり、ビジネスプロセスを変革したりしています。欧州委員会は、大部分のデータの作成や収集、処理、保存の対象は個人情報であり、EU域内のデータ主体に関する様々な情報が公開されるリスクがあることを認識していました。

データの保護に関する従来の規制は、個人情報の保護や安全性に対する懸念を必ずしも軽減するものではありません。データの保護に関する規制がEU加盟国全体で統一されていないことに、データ主体である市民は不満を感じています。実際、90%もの人が、データの保存や処理が行われる場所に関係なく、EU全体で同じ規制を適用してほしいと考えています。*

こうした状況を受け、デジタル時代を生きる人々の基本的なプライバシー権の保護を強化し、統一性がない現在のデータ保護法に対する懸念を払拭する目的で、GDPRが制定されました。

2018年5月にGDPRが施行されると、企業の多くには、顧客や市民、従業員などのデータをこれまでより効果的に管理し保護する義務が発生します。この規制は、国籍や居住地を問わず、EU域内にいるデータ主体を対象とし、個人情報の保護に関する原則や規則を示します。

GDPRは「原則」ベースの法規制のため、企業は自社のビジネスに固有の状況やデータの用途を踏まえて、果たすべき義務とそれ以外の義務を見極めなければなりません。企業がGDPRに対する取り組みを主導し推進していくためには、これらの原則を理解しておく必要があります。

GDPRでは、新たに定められたデータプライバシーの原則を遵守するため、現在と将来の情報資産の利用状況を詳しく把握することを求めています。多くの企業では、従業員、プロセス、テクノロジー、データ管理のプラクティスやポリシーに影響すると考えられます。

違反した場合は、その種類や規模に応じて多額の罰金が科せられる恐れがあります。違反企業には、最高2,000万ユーロまたは世界売上高の4%のうちいずれか高い方の金額が制裁金として科せられます。

2.2 GDPRの対象

GDPRへのコンプライアンスには様々な側面があり、地理上の場所で制限されることはありません。北米やアジアなどの企業も、EU域内の個人の情報を保存、処理する場合はこの規制を遵守する義務があります。個人情報を取り扱う事業者は、消費者と直接取引する企業（B2C）、他の企業・組織と取引する企業（B2B）、データ処理専門企業ですが、オペレーションセンターやデータセンターの所在地に関係なく、EU域内のデータ主体に関する情報を取り扱う企業は、コンプライアンス要件をもれなく理解する必要があります。

* http://ec.europa.eu/justice/data-protection/reform/index_en.htm

2.3 GDPRの対応に伴うデータに関する課題

GDPRの施行に伴い、多くの企業には、データについて明白な課題がもたらされます。GDPRへのコンプライアンスを実現するには、企業内のどこで個人情報が使われていようと、そのデータの制御とガバナンスを確保しなくてはなりません。しかし、企業やそのビジネスエコシステムの至る所にデータが蔓延しているため、データ管理は難しくなっているのが現状です。データの多様化やクラウドコンピューティングへの移行といった顕著なトレンドによって、非常に動的なIT環境が生まれ、データ管理やセキュリティに関する課題が増えています。こうした課題を分かりやすく示すため、GDPRに関連して多くの企業が簡単に答えを出すことができない質問を下記に紹介します。

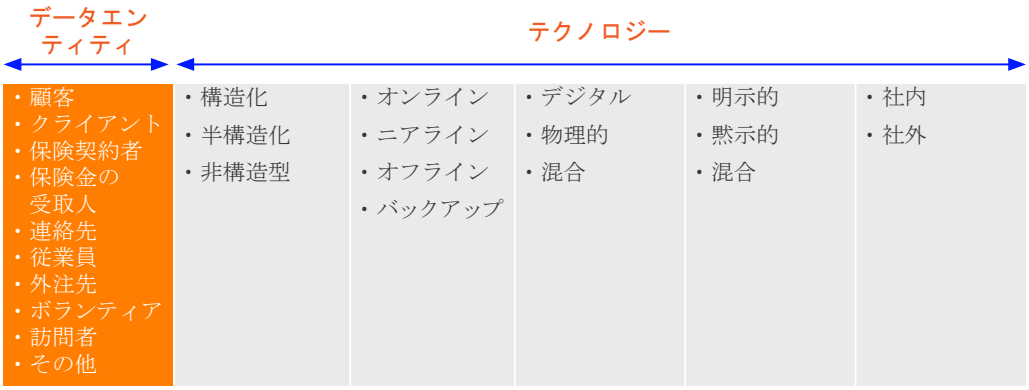
- GDPRの原則が適用される対象データは、社内や自社エコシステムのどこにありますか？それらのデータは危険にさらされていますか？
- どのような方法で、ビジネスエコシステムにあるデータを追跡していますか？
- 必要なポリシーと手順がすべて適用され、確実に実施されるように、自社のデータ資産をどのように定義し管理していますか？
- GDPRの原則が適用される対象データレコードは、社内のどこに保存されていますか？こうしたデータレコードはどのように特定し、関連付けることができますか？
- どのようにデータ主体から同意を取得し、その同意を管理していますか？データ主体の同意内容に対する変更や同意の定義をどのように管理していますか？
- データ主体からのアクセス要求、削除権、移動要求に対し、どのような方法で指定期間内に効率的かつ効果的に対応できますか？
- 関連データへのアクセスをどのように制御していますか？自社の業務機能や活動に必要ない場合、個人情報を削除していますか？

2.4 規制の対象になりうるデータの種類

考えられるもう1つの課題は、企業が保持しているデータの種類に応じてどのような対処を行うかという点です。ここでは、下記に2種類の定義を紹介します。

1. データエンティティタイプ
2. データエンティティタイプを管理するテクノロジータイプ

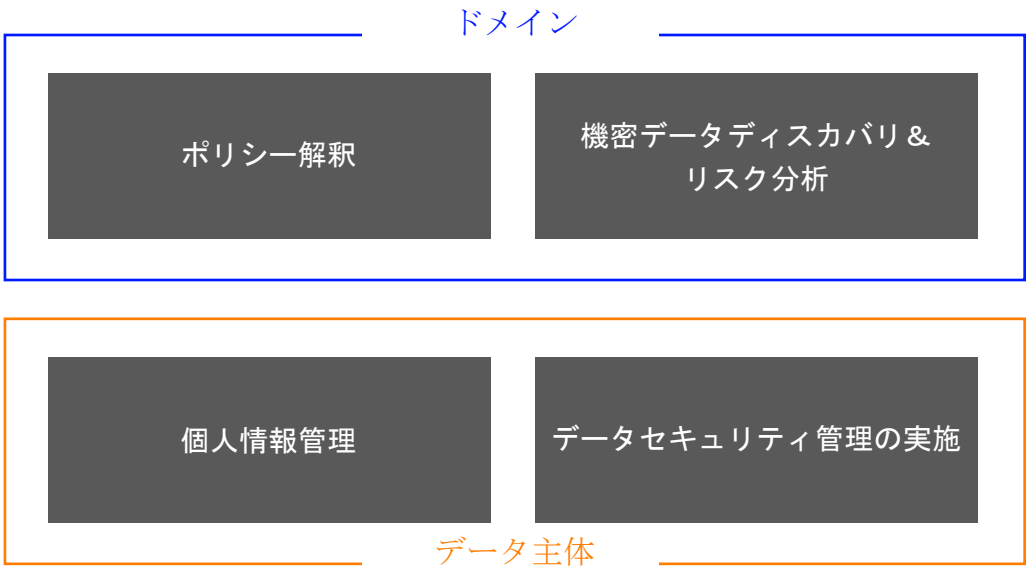
データ主体の情報の大半は、1つまたは複数のデータエンティティタイプだけでなく、1つまたは複数のテクノロジータイプにも属します。下の図には、データタイプとテクノロジータイプのなかで、GDPR対象データに適用される可能性があるタイプをまとめています。



異なる種類が存在することで、GDPR対象のデータ資産を取得、管理する場合に別々のアプローチや手法、テクノロジーを採用しなくてはならない場合もあります。

3.エントリーポイント、必要な機能、テクノロジーの使用事例

インフォマティカは、GDPRの対応に関する課題について理解や認識を深めてスムーズに行動計画を作れるように、データの共通課題を浮き彫りにするエントリーポイントの質問を規定しました。多くの場合、単純な質問を使うことで、エントリーポイントの作業を進めることができます。質問によっては、従業員やプロセス、テクノロジーについて慎重に検討してから回答しなくてはならないものもあります。答えを見つけやすくするために、必要な機能とその機能を実現するテクノロジーの使用事例をまとめました。必要な機能はグループ化しています。以下の図では、このグループ構成と各グループの関連性を示しています。



各機能は、ドメインとデータ主体という2つの領域に分かれています。

ドメインは、データ主体のデータドメインに関連しています。ドメインの探索や管理に関するインサイトを引き出し、適用範囲の定義やデータの構成ビューの提供に使用されます。

データ主体は、トランザクションレベルにあるデータ主体の実データに関連しています。個人情報管理に関するインサイトを引き出し、データ主体レベルの対応やインサイトを提供する場合に使用されます。

3.1 エントリーポイントの質問：対象になりうるすべてのデータはどこにあるか？

背景：一般的に、データはエンタープライズ環境全体で使用している様々なシステムやアプリケーション、ソースに分散しています。この状態は、特に大企業、買収で成長してきた企業で見られます。EU域内のデータ主体が企業で果たす役割（顧客、サプライヤー、パートナー、従業員など）を考えると、個人情報が1つの部門やシステムだけにとどまる可能性は低いといえます。多様なITシステムが存在する企業では、コアのアプリケーションにあるデータだけでなく、スプレッドシートやローカルデータベース、ビッグデータソリューションのデータも考慮する必要があります。

必要な機能：機密データのディスカバリおよびリスク分析は、幅広いテクノロジーソリューションからデータを探索する機能です。実データや蔓延したデータの量などを他の情報ソースと組み合わせて、データのリスクスコアを作成します。リスクスコアから最もリスクが高いデータの保存場所を把握できるため、リスクに基づいて改善措置やセキュリティ管理要件の優先順位を決定できます。一定期間にわたってリスクスコアを追跡することで、改善措置や管理対策がデータのリスク軽減に効果を発揮しているかどうかを確認することが可能になります。法律上の目的で同意が必要になる場合は、データリネージなどの機能を使用して個人情報の新たな保存場所を特定し、利用に対する潜在的な変更を把握できます。

テクノロジーの使用事例：機密データのディスカバリおよびリスク分析は、検出機能に焦点を当てた検出と保護の使用事例として位置付けることができます。規制の対象となる機密データの場所やそれらが蔓延している場所に関するインサイトと、データのリスクに対する分析的なインサイトを提供するコア機能です。この使用事例には、以下のように一般的な機能を適用することが可能です。

- **データポリシー定義**業務部門とIT部門の定義、不明確なデータ、ポリシーの衝突
- **データディスカバリの自動化**：対象となる機密データの検出、最初のデータ受け渡しと継続的な監視、データの分類、サポートシステムの統合
- **データの蔓延**：データはどこにあるか？それはどこに行くのか？新しいソースか？
- **データのリスク評価**：データの移動+蔓延+アクセス+量に基づく優先順位付け。計画、履歴、一定期間にわたるスコアの監視
- **データの保護**：データのアクセス制限が必要な場所、匿名化すべきデータ、暗号化の適用先、時間／場所／役割別のデータ閲覧を特定

テクノロジーソリューション：**Informatica Secure@Source**は、対象データの保存場所の探索やデータの分類、蔓延するデータの監視やリスクスコアの割り当てに活用できます。一定期間データを追跡することによって、変更がコンプライアンス活動にプラスの影響またはマイナスの影響を与えているかどうかが分かります。

利点：データの場所だけでなく、リスクに応じたデータのランク付けについてのインサイトを得ることができます。

3.2 エントリーポイントの質問：個人情報をどのように使用しているか？

背景：世界は今、デジタルトランスフォーメーションの真っ只中にあります。そして、この状況はあらゆる分野に影響を与えています。生成、収集、分析対象のデータの増加は世界中で起きている現象であり、こうしたデータの大半は個人情報に属する可能性があります。企業にデータが蔓延するのに伴い、データに対する責任の所在を明確にし、データを制御、管理することが以前より難しくなっています。様々な法規制へのコンプライアンスと同様に、GDPRへのコンプライアンスもデータガバナンスに対するアプローチを全社に導入することで最適な形で実現できます。

必要な機能：ポリシー解釈は、ポリシー、責任、プロセス、データ用語、論理モデルと物理モデルを、ビジネスとテクノロジーの両方の観点から理解するための機能です。重要なのは、技術環境の理解とビジネス環境の理解を関連付ける機能でもあるという点です。こうした関連付けの機能は、対象となるデータドメインの情報について総体的なビューを提供し、データ資産の管理アプローチに欠かせない役割を果たします。

テクノロジーの使用事例：ポリシー解釈は、企業データのガバナンスの使用事例として位置付けることができます。企業でのデータ管理についてトップダウンとボトムアップのビューを提供し、業務部門とIT部門の情報ビューを結び付けるコア機能です。この使用事例には、以下のように一般的な機能を適用することが可能です。

- **ポリシーの定義**：業務部門とIT部門の定義、すべての業務レベルのドキュメント、論理データと物理データ、プロセスモデル
- **責任**：データの所有者は誰か？データを使うのは誰か？品質とセキュリティに関する責任者はどの部門か？
- **用語とプロセスの定義**：ビジネスプロセス、主なデータエンティティ、属性、システム、品質管理、標準化、ビジネス上の同意の定義
- **変更プロセス**：定義のための統制プロセス、変更のための統制プロセス、プロセスガバナンス
- **アーチファクトとの関連付け**：論理アーチファクトと物理アーチファクトの関連付け、技術面とビジネス面でのデータリネージ、データ品質の統合

テクノロジーソリューション：業務部門とIT部門がデータガバナンスの共通のゴールに向けて連携できる、エンタープライズデータガバナンスソリューションを導入します。**Informatica Axon**のようなデータガバナンスソリューションは、業務部門とIT部門のデータビューを統合する目的で設計されており、論理データ資産と物理データ資産の関連付けを行います。

利点：企業のプロセス、ポリシー、データエンティティを定義する際に、あらゆる分野の専門家から簡単かつ手軽に支援を受けることができ、規制対象のデータについて総体的なデータガバナンスを短期間で確立できます。

3.3 エントリーポイントの質問：データ主体の情報をどのように管理しているか？

背景：複雑なIT環境でデータの利用が多様化した結果、データ主体のすべての情報を把握できる単一のビューを確立することが困難になってきています。こうした問題の原因は、データの保存やインデックス化がシステムごとにまったく違うメカニズムで行われているところにあります。データ主体の情報に加え、企業での情報の保存、管理、処理を把握できる包括的なビューがなければ、GDPRへのコンプライアンスの確保、特にデータ主体の権利の保護は難しくなるでしょう。

必要な機能：個人情報管理は、特定した全ソースからデータ主体のレコードを発見し、それぞれのデータ主体とレコードを照合して関連付けを行い、Entity 360のリポジトリを作成する機能です。このリポジトリには、規制対象のソースに保持されている実際のデータレコードや各データとデータ主体との関連付けについて、高品質のデータが集められています。Entity 360は、企業がデータ主体からのアクセス要求、削除権、移動要求へ対応する場合に、信頼できるデータソースとして利用できます。ビジネス上の観点で見ると、Entity 360は個人情報の用途に関する同意の管理をサポートします。さらに、「どのチャネルを介して、いつこの同意が取得または取り消されたか？どのような条件に同意したか？」といった同意の内容も管理できます。

テクノロジーの使用事例：個人情報管理は、データ照合と関連付けの使用事例として位置付けることができます。様々なシステムからデータ主体のレコードを発見し、同種レコードの照合や関連付けによってシステム間のデータビューを提供するコア機能です。この使用事例には、以下のように一般的な機能を適用することが可能です。

- **関連データへのアクセス**：データ主体の情報のプロファイリング、ソースシステムからの関連データ抽出、半構造化コンテンツや非構造化コンテンツへの分析プロセスの適用
- **データ品質プロセス**：データ品質レベルの評価、手動／自動による改善措置、手動による改善措置のプロセス管理、評価基準に基づくレポート作成
- **同意の内容、同意の取得方法や管理方法など、データ主体に関する情報の信頼できる単一ソース**：データ主体の同意内容に基づいて、異なるビューや視点が反映されます。
- **照合と関連付け**：ビジネスプロセスの定義に基づくマッチングルールの定義、レコードの照合、同種レコードとスコアリングの関連付け、同意の関連付け
- **データ永続性**：永続的な関連付けの対象／対象外のレコード、アナリティクス、レポート

テクノロジーソリューション：高度なアルゴリズムを利用して、データの保存場所を問わず、同じデータ主体の全データを照合し、すべてのデータドメインからこのデータ主体のレコードを探索できるソリューションを導入します。**Informatica Relate 360**では、高度なアルゴリズムを使うことで、同じデータ主体に関連付けられているデータを特定します。マスターデータ管理は、データ主体の情報を示す共通ビューを確立し管理するためのフレームワークを提供します。

利点：個人の単一ビューは、GDPRへの対応以外にも様々なビジネス上の利点をもたらします。対象の個人が顧客の場合、特に大きなメリットがあります。個人顧客は、自分に合わせてカスタマイズされた体験を期待するようになっているためです。GDPRへの対応という観点から見ると、各データ主体の情報をすべて関連付けできることで、個人の権利の行使という負担が軽減されます。データの用途の理解、忘れられる権利の行使、同意の適切な適用などの面でも利点があります。

3.4 エントリーポイントの質問：どのようにデータを保護し、不正アクセスを防止しているか？
背景：データ保護の管理は、GDPRで定められた同意に関する要件に従い、個人情報の保護を支援するアプローチです。テスト目的で使用する運用データを削除やマスキング、匿名化するようにIT部門が要求する場合もあります。あるいは、外部へ転送するデータの匿名化が求められることもあります。コンプライアンス確保のためには、アプリケーションでユーザーに適用している個人情報へのアクセスコントロールを見直す必要があります。

必要な機能：**検出と保護**も、データ主体の情報にアクセスコントロールを適用し、個人情報を守ります。多くの場合、データ主体の情報は、企業やそのエコシステムの中で様々な担当者に公開されます。データセキュリティ管理は、こうした情報を削除したり、閲覧すべきではない担当者から隠したりするために使用しますが、必要な担当者に情報を提供する目的でも使用します。

テクノロジーの使用事例：同意の管理は、検出と保護の使用事例として位置付けることができます。これは、データマスキングや暗号化、アクセスコントロールなどのデータ中心の制御を適用して、データへのアクセスを保護したり、データやアプリケーションのアーカイブや削除といったデータライフサイクルを管理したりするためのコア機能です。この使用事例には、以下のように一般的な機能を適用することが可能です。

- **リスク分析へのインプット**：リスク評価に基づいてデータ管理方法を提示します。
- **オーケストレーション**：特定されたリスク、安全ではないアクセスや状況の監視結果に基づいて、データの保護タスクのスケジュールを設定、調整する機能
- **データセキュリティ管理**：静的または動的なマスキング、匿名化、役割ベースのアクセス、暗号化、トークン化
- **変更履歴／更新履歴**：ソースシステムに対する適用、レコードマスキングまたは同意レコードとの照合結果のアーカイブ、監査証跡の生成
- **アーカイブ**：運用システムからのデータのアーカイブ、証拠を残すログアクティビティ、偶発的な使用やアクセスを防ぐためのオフライン移行

テクノロジーソリューション：データ資産のライフサイクルを管理し、データ資産を制御するソリューションを導入します。**Informatica Persistent Data Masking**と**Informatica Dynamic Data Masking**では、個人情報に制限なくアクセスできるユーザーやシステムの数を自動的に調整します。**Informatica Secure@Source**は、セキュリティ対策へのアップデートを調整することによって、データセキュリティの改善措置を提供します。

利点：データマスキングを自動化し、個人情報保護違反のリスクを軽減します。個人情報は閲覧を許可されたユーザーだけがアクセスできるようになり、適切な保護対策がないまま個人情報が蔓延することはありません。

4.パートナー

様々な法規制やコンプライアンスと同様に、テクノロジーだけでコンプライアンスを確保することはできません。企業がGDPRへのコンプライアンスを実現するには、従来のサービスやテクノロジーソリューションだけでなく、最適なソートリーダーの存在も大切です。インフォマティカは、企業の幅広いGDPRイニシアチブをサポートできるよう、適切な教育を受けた高いスキルを持つパートナーとの協力体制を確立しています。データ管理に精通し、GDPRへのコンプライアンスに重点的に取り組んでいるパートナーが選ばれています。

貴社にとって最適なパートナーはこちらでお探しいただけます。または、インフォマティカまで直接お問い合わせください。お客様のニーズや要件に合わせた最適なパートナー探しのお手伝いをさせていただきます。

5.結論

このホワイトペーパーでは、GDPRの施行がデータに及ぼす影響を検討し、理解する必要性を説明しました。この新しい規制は、多くの企業に課題とチャンスの両方をもたらします。GDPRの発効まで残された時間はあとわずかです。GDPRの原則を理解することで現在および将来のデータ管理プロセスがどのように変わるのかを、企業は考える必要があります。

こうした原則を速やかに業務へ反映できるように、このホワイトペーパーでは関係者から寄せられる主なエントリーポイントの質問を紹介すると共に、これらの課題を解消するために必要な機能を提案しました。これらの質問や機能は、GDPR要件のごく一部に対応するものではなく、GDPRによって生じるデータの課題を解決するための包括的な機能の構築に役立ちます。

テクノロジーの使用事例は、それぞれの機能に応じて示しています。各使用事例では、その実現に際して導入可能なソフトウェアソリューションやテクノロジーの種類をまとめました。

20年以上にわたりデータ管理ベンダーとして業界をリードしているインフォマティカは、世界中の様々な企業が抱えるデータ管理の課題を解消しています。GDPRの施行により、多くの企業がデータ管理に関する複雑な問題に直面するでしょう。しかし。インフォマティカとパートナーで構成されているエコシステムが、GDPRへの対応に取り組む企業に最適な支援を提供します。

6.免責事項

GDPRへのコンプライアンスは、各社の事業内容や業務、データの利用法といった具体的な事実が基盤になります。このドキュメントは、各社がGDPRへのコンプライアンス体制を固めていく上で役立つと考えられる論点を提供するものであり、法的なアドバイス、ガイダンス、推奨事項を意図したものではありません。各社が履行すべき義務や履行が不要な義務については、それぞれの法律顧問に相談してください。

Informatica

〒105-6226 東京都港区愛宕2-5-1 愛宕グリーンヒルズMORIタワー26階 電話：03-6403-7600(代表) FAX：03-3433-1021
www.informatica.com/jp linkedin.com/company/informatica twitter.com/Informatica

IN09_0218_03337