GDPR

Creating Value with General Data Protection Regulation

La visión de IBM

LOGICALIS

Barcelona, 14 de Febrero

Los clientes son responsables de garantizar el cumplimiento de las leyes y normativas aplicables, incluyendo el Reglamento General de Protección de Datos de la Unión Europea.
Los clientes son los únicos responsables de obtener asesoramiento legal competente a fin de identificar e interpretar cualquier ley y normativa que pudiera afectar a su negocio, así como cualquier medida que debieran tomar para cumplir con dichas leyes y normativas.
Los productos, servicios y otras funcionalidades descritas en este documento no son los indicados para todas las situaciones del cliente y podrían estar sujetas a disponibilidad.
IBM no proporciona asesoramiento legal, de contabilidad ni de auditoría, ni declara ni garantiza que sus servicios o productos son garantía de que los clientes cumplen con las leyes o normativas vigentes.

Disclaimer

- **Notice:** Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsibility for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

- Any statements about project durations and prices are estimations without any legally binding effect and are subject to change or withdrawal without notice at IBM's sole discretion.

None of the statements contained herein constitutes legal guidance – it is process guidance only.

Pero …. ¿de qué va realmente GDPR?

5 áreas clave de actuación …

que impactan en todos los ámbitos de la organización

Gobierno

Personas, Comunicación & Reporting

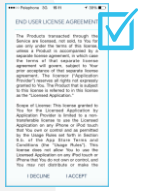
Procesos

Gestión de Datos

Seguridad

Marco general de adecuación: Ciclo de vida

Gestión del Consentimiento
- Obtención y
- Registro Histórico de cambios. No repudio
- Autoservicio para la gestión



Trazabilidad sobre los datos
- Quién
- Por qué / Para qué
- Cuándo / Dónde

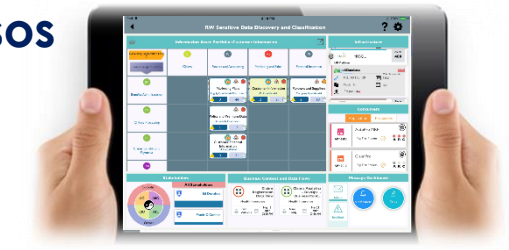
Concienciación

Descubrimiento de datos
- Categorías de datos (multiidioma)
- Repositorios estructurados/ no estructurados y físicos
- Biblioteca de filtro de datos

Datos / Repositorios

Evidenciar

Procesos



Gobierno / Dashboard

Tratamientos

Registro de Tratamientos

Análisis de Tratamientos
- Finalidad / Legitimación
- Información al titular
- Cesiones / transferencias
- Encargados / Proveedores
- Ciclo de vida / flujos

"Por defecto" y "por diseño"

Gestión de derechos ARCO + PL
- Acceso, Rectificación, Supresión ("olvido"), Oposición
- Portabilidad y Limitación de Uso

Ejecución de Derechos (Gobierno Dato)
- Catálogo
- Visión integrada de los datos
- Múltiples repositorios/entornos

Gestión de brechas de seguridad
- Registro de incidentes
- Coordinación con áreas de seguridad
- Auditoría & Forensics
- Resolución & Capitalización

Riesgos

Registro de Riesgos / EIPDs

Análisis de Privacidad …
- Derechos y Libertades
- Análisis de Impacto sobre Privacidad

Medidas de Protección

Monitorización actividad de ficheros y bases de datos

Protección Auditoría, Monitorización y Trazabilidad

Protección

Bloqueo dinámico

Seudonimi-zación

… y de la Seguridad
- Bases de Datos
- Aplicaciones
- Infraestructuras

Funcionalidades tecnológicas necesarias

GDPR
EU General Data Protection Regulation

Decisión Tecnología

Madurez GDPR → Inventario → Transformación → Mantenimiento/ Operación

Gobierno, gestión del cambio, proceso

- Inventario de conformidad – Registro de tratamiento & Plan de remediación/PIAs, Conservación de datos

Datos personales: análisis de riesgos y proceso de tratamiento

- Cartografía de datos personales
- Descubrimiento datos no estructurados
- Descubrimiento datos estructurados
- Cartografía de Datos & Borrado, Portabilidad
- Anonimización / enmascaramiento
- Cifrado
- Supresión / Puesta en cuarentena
- Restitución/Transfererencia/Rectificación

Seguridad y Protección operacional

- Seguridad Operacional del Sistema de Información
- Protección operacional de los datos
- Control de actividad de usuarios, permisos
- Gestión de incidentes

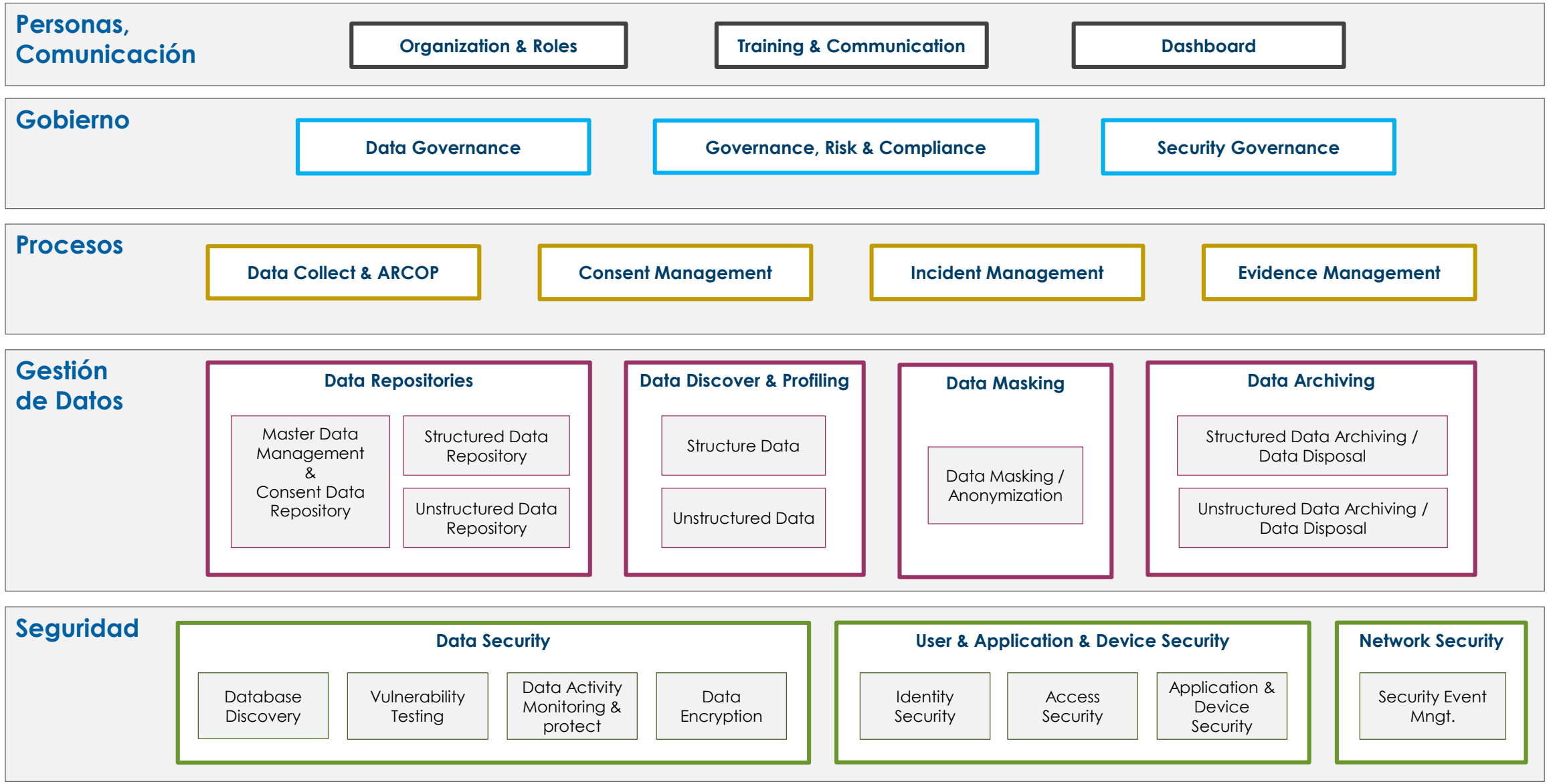
Consentimiento

- Gestión del consentimiento

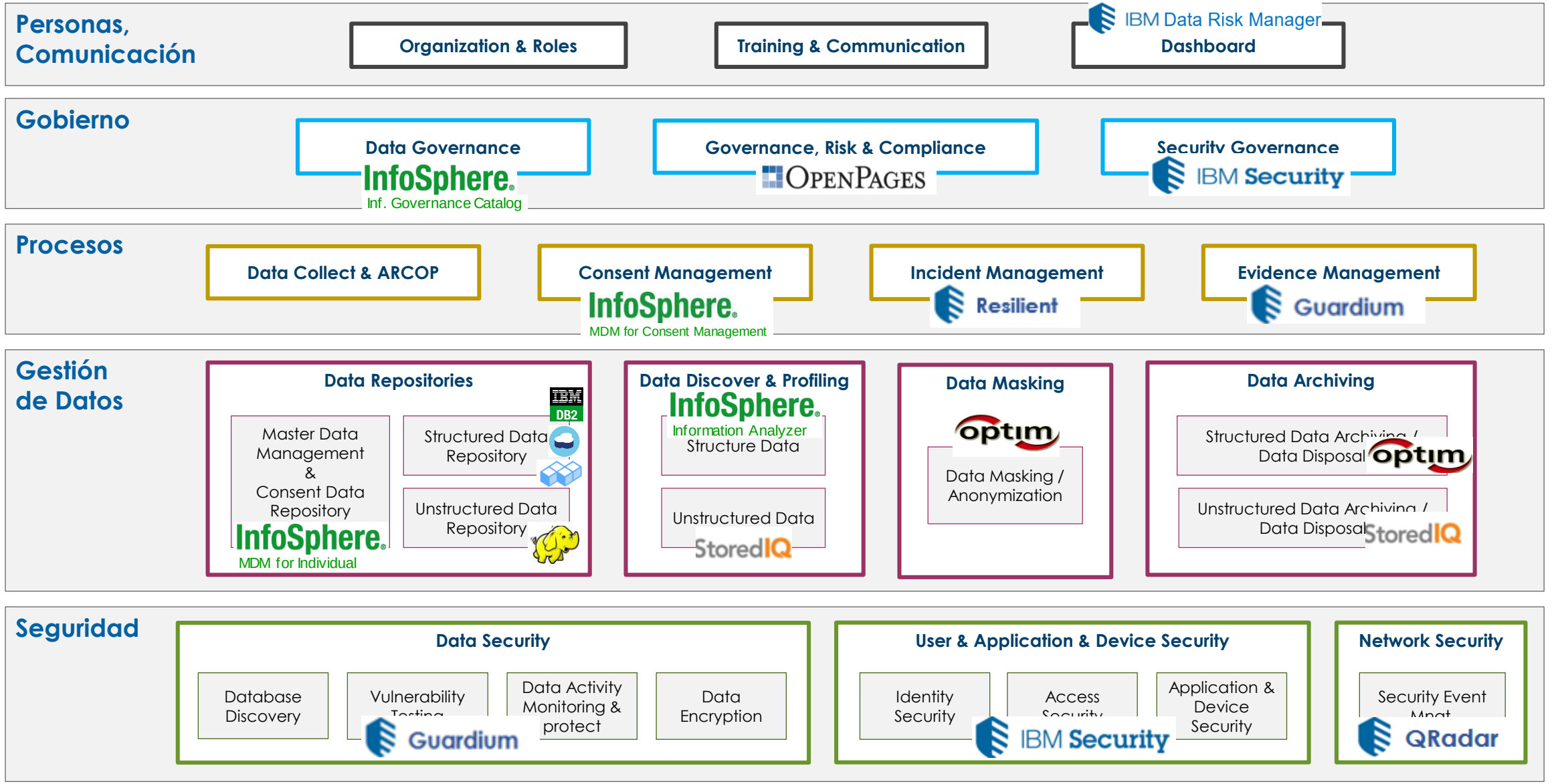
Privacidad por Diseño/ por defecto

- Base de datos
- Aplicaciones
- Infrastructura / Movilidad

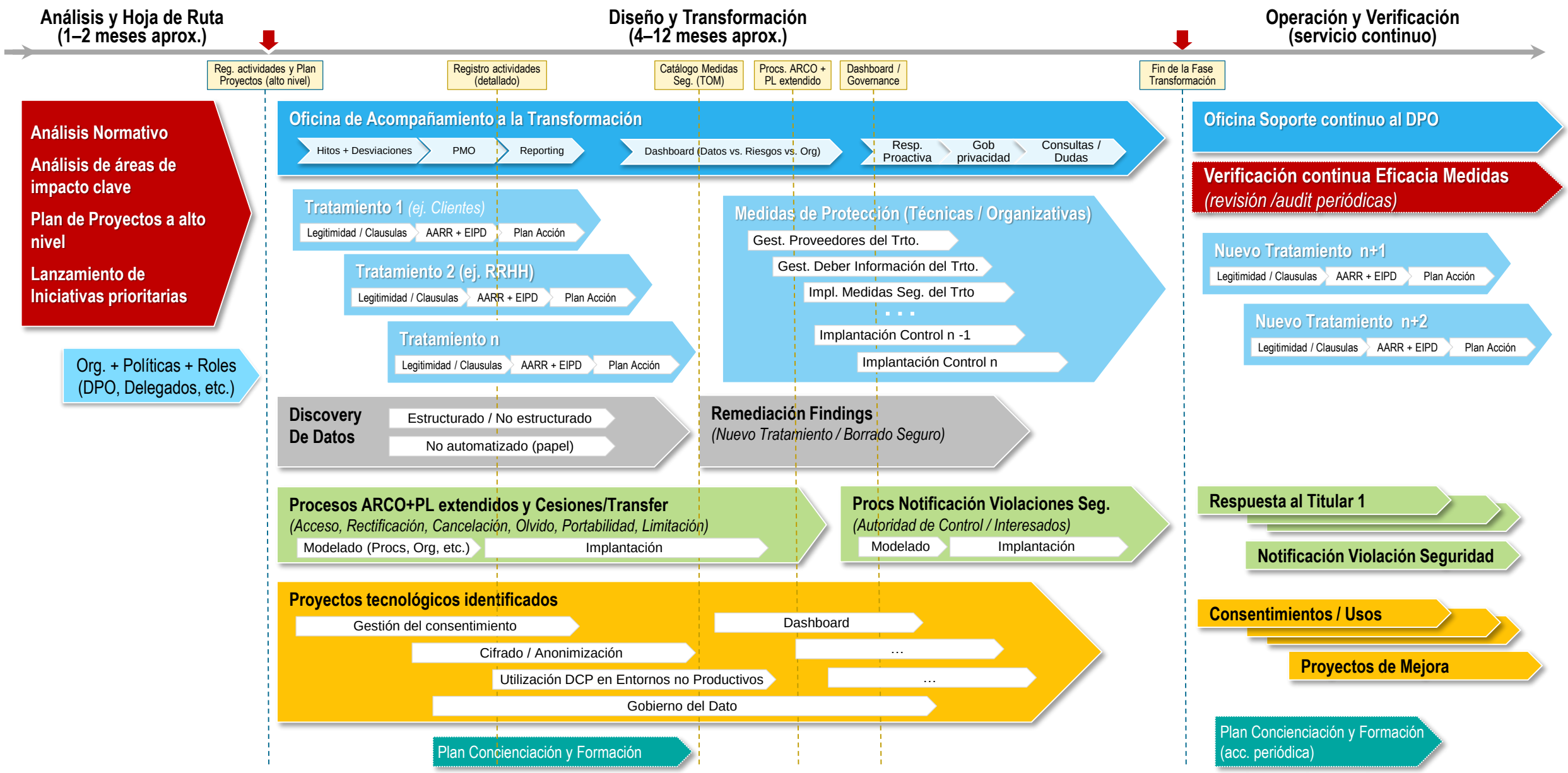
Arquitectura de Referencia Funcional para GDPR



Arquitectura de Referencia Funcional para GDPR



Proyecto GDPR: Roadmap global y metodología de trabajo

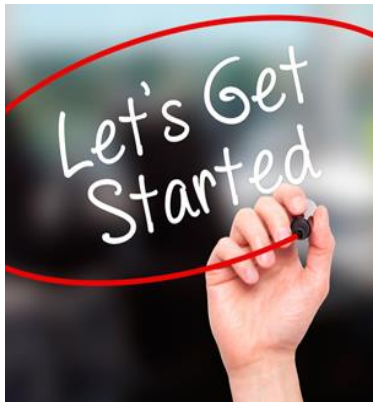


Principales líneas de actuación: “Building Blocks”

Análisis de Tratamientos → Análisis de Riesgos y PIAs → Definición de Procesos → Medidas de Protección → … → Resporting y Control

Es necesario arrancar cuanto antes !!

- Y para comenzar, hay 4 puntos clave de actuación:



Análisis Regulatorio GDPR → **"Data Risk Dashboard"** → IBM Data Risk Manager

Localizar los Datos

- Descubrir, localizar y entender donde está la Información Sensible / Pºersonal.
- Estructurados y No Estructurados.

InfoSphere
Information Analyzer
Governance Catalogue

StoredIQ

Asegurar los Datos

- Monitorizar accesos: Quién, Qué, Cuándo.
- Securizar los datos: bloqueo, cifrado, etc.
- Vulnerabilidades en repositorios

IBM Guardium

Gestión Consentimiento

- Captura
- Granularidad
- Propósito / Finalidad
- Derechos ARCO

InfoSphere
MDM for Consent Management

GDPR

Creating Value with General Data Protection Regulation

Gracias por su atención

LOGICALIS

Los clientes son responsables de garantizar el cumplimiento de las leyes y normativas aplicables, incluyendo el Reglamento General de Protección de Datos de la Unión Europea.
Los clientes son los únicos responsables de obtener asesoramiento legal competente a fin de identificar e interpretar cualquier ley y normativa que pudiera afectar a su negocio, así como cualquier medida que debieran tomar para cumplir con dichas leyes y normativas.
Los productos, servicios y otras funcionalidades descritas en este documento no son los indicados para todas las situaciones del cliente y podrían estar sujetas a disponibilidad.
IBM no proporciona asesoramiento legal, de contabilidad ni de auditoría, ni declara ni garantiza que sus servicios o productos son garantía de que los clientes cumplen con las leyes o normativas vigentes.

1. Localización y Descubrimiento de Datos Personales

InfoSphere
Information Analyzer
Governance Catalogue

StoredIQ

GDPR Outcome

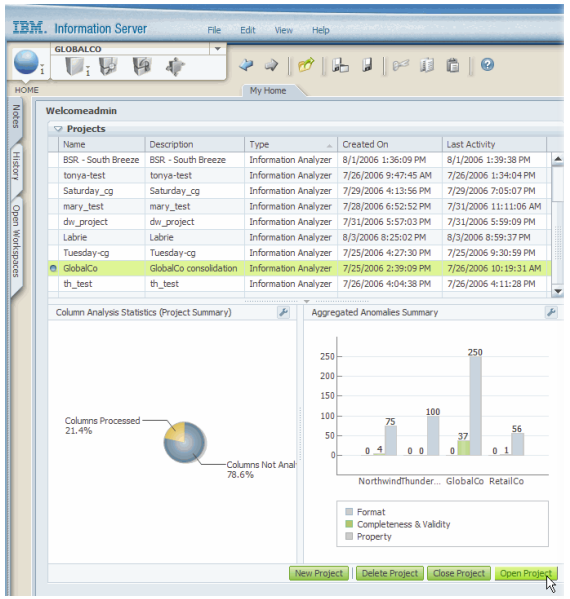
Rapidly discover the most common Personal data in all the usual places, avoiding internal time and resources trying to define and manage these rules; Ensuring IT can help other stakeholders reduce Risk and Cost of Discovery.

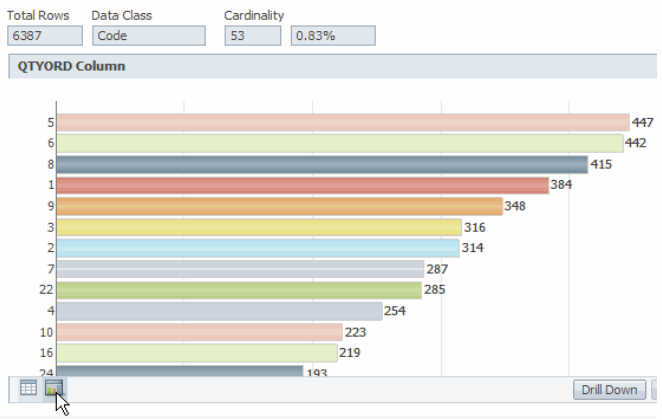
Plug-in discovery accelerators to find a more extensive set of EU citizen personal data

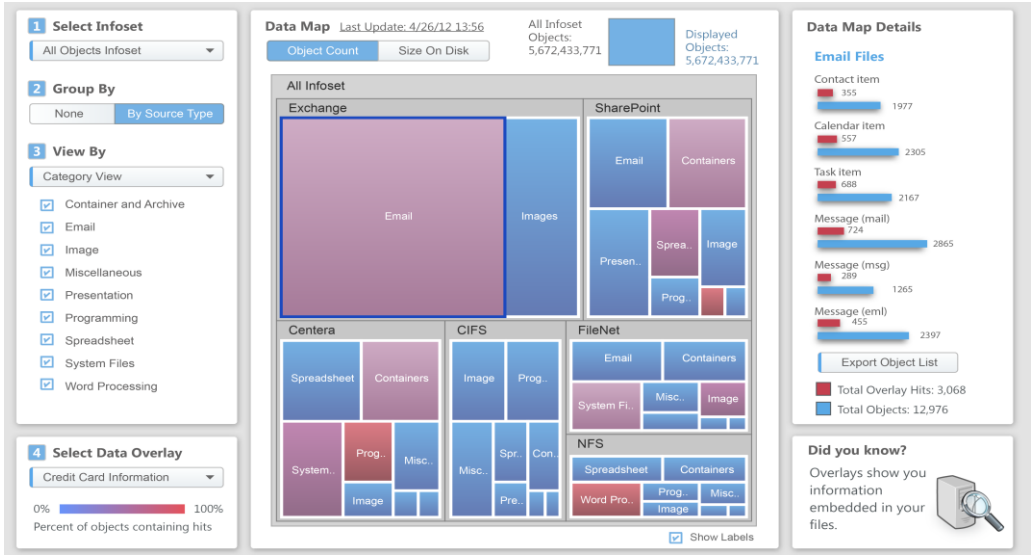
- Maximising the use of RegEx strings
- Leveraging Machine Learning Annotators to auto-discover personal data *entities* such as Names, Addresses, Countries that can't be defined or found by RegEx
- Tailorable & extensible by clients

Proven enterprise-scale capability to assess in-place the common sources and types of unstructured information

- Heatmap view to prioritise Where Personal information has been found
- Actionable outcomes and exports of specific data types and files for remediation & mapping







2. Aseguramiento de los Datos Personales

IBM Guardium

GDPR Outcome

Monitor and audit access to personal data, detection and alerting of non-compliant access.

IBM® Security Guardium® Data Activity Monitor prevents unauthorized data access, alerts on changes or leaks to help ensure data integrity, automates compliance controls and protects against internal and external threats.

Continuous monitoring and real time security policies protect data across the enterprise, without changes or performance impact to data sources or applications.

Guardium Data Activity Monitor protects data wherever it resides, and centralizes risk controls and analytics with a scalable architecture that provides 100% visibility on data activity.

It supports the broadest set of data source types, and it is the market leader for big data security solutions.

- Monitor and audit all data activity—for all data platforms and protocols.
- Enforce security policies in real time—for all data access, change control and user activities.
- Create a centralized normalized repository of audit data—for enterprise compliance, reporting and forensics.
- Support heterogeneous data environments—all leading databases, data warehouses, files applications and operating systems, including big data environments (Hadoop and NoSQL).
- Feeds into QRadar , to allow correlation of data repositories and content store access events with infrastructure and application for a holistic view of system access.

Base de conocimiento predefinida mapeada con las obligaciones GDPR (Artículos) que incluye:

- Descubrimiento y clasificación de datos personales
- Identificar y remediar vulnerabilidades
- Informes de monitorización y auditoría en tiempo real para datos personales GDPR
- Políticas y grupos predefinidos para datos personales GDPR
- Flujos de procesos para cumplimiento
- Paneles para auditores, controllers y DPOs

How do I help meet GDPR Article 32, *Security of processing?*

Encrypt personal data with Guardium Encryption

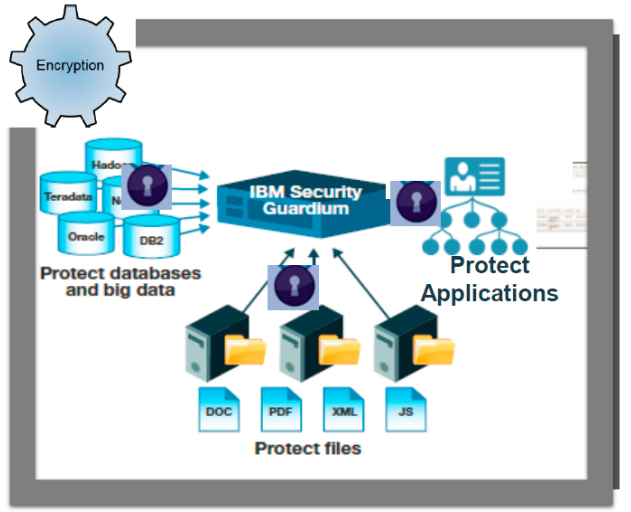
On Prem: Guardium Data Encryption

- DBs and big data platforms
- Files and folders
- Applications
- Supports separation of duties

On Cloud (NEW!): Guardium Multi-Cloud Encryption (MDE) http://ibm.biz/Bds7jt

- Safeguards data from misuse on single cloud, multiple clouds, or hybrid environments

For Key Management: IBM Security Key Lifecycle Manager (SKLM) securely distributes keys across complex encryption landscapes



3. Gestión del Consentimiento

InfoSphere
Consent Manager Asset

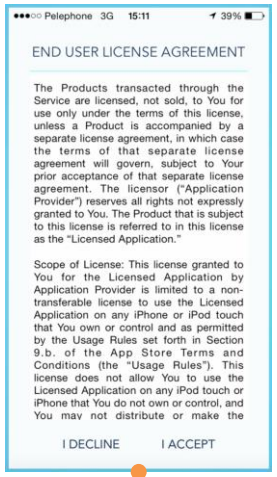
MDM for Consent Management

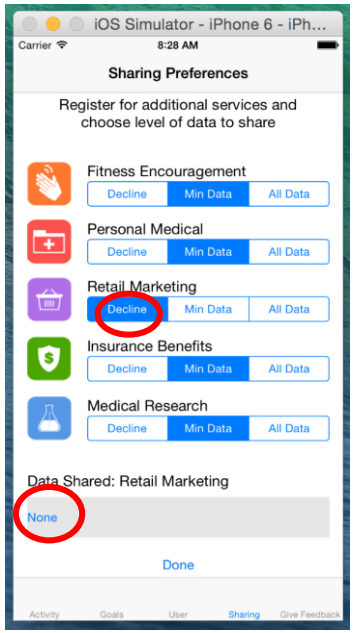
GDPR Outcome

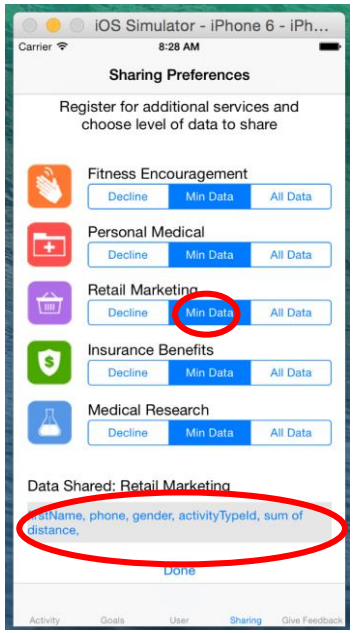
Where required, explicit transparent Purposeful Consent of any personal data categories is available for citizen and processors to trust and understand how it can be and is used.

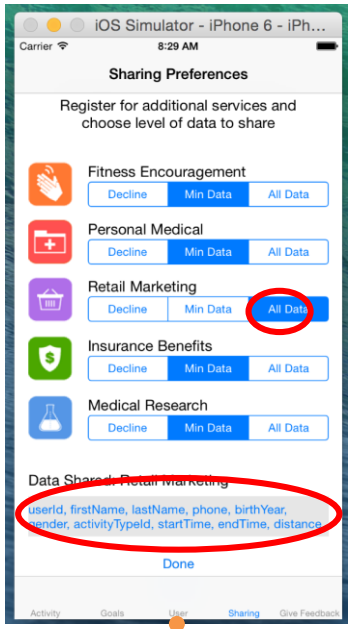
Consent Service providing framework for obtaining, maintaining and applying where specific consent is required for some GDPR data processing, away from the current blanket single consent commonly imposed.

Supports any categories of Consent or Sharing preferences for citizens, flexible and changeable by them at any time. Each is more granular, specific for each Purpose and clearly conveys What data is related to that consented purpose.





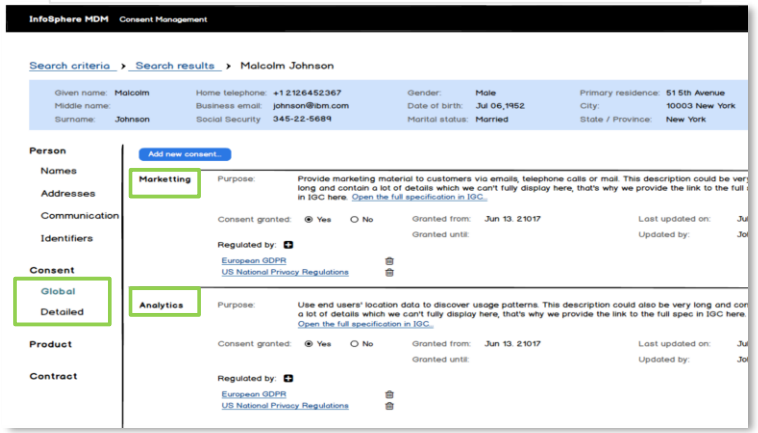




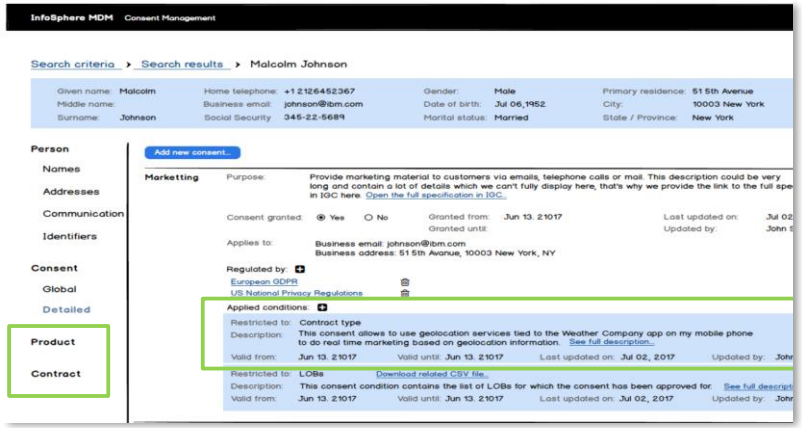
A Consent Management Solution hence is comprised of 3 building blocks:

- Define GDPR including consent
- Capture and maintain consent for individuals
- Enforce consent in application systems

Grouping of global vs. detailed consent, by consent type, consent type hierarchies and/or combinations

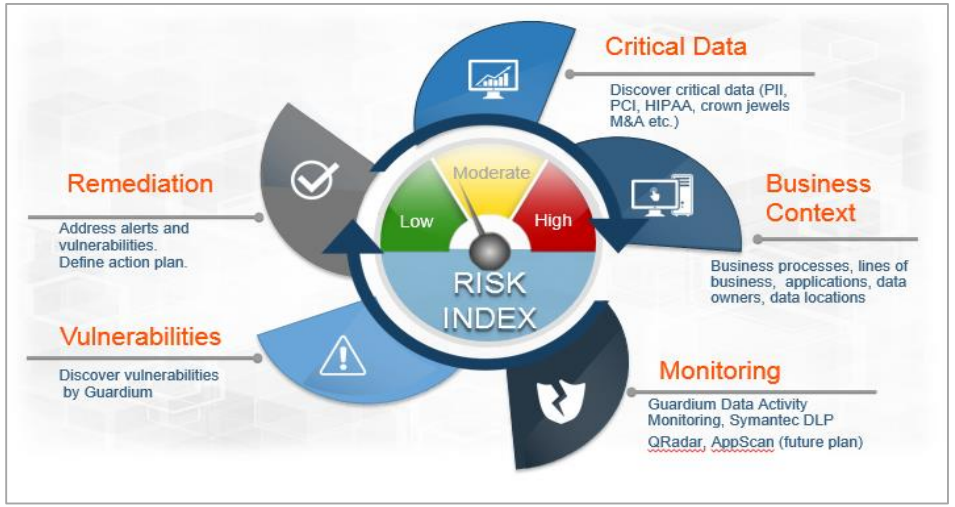


Grouping of global vs. detailed consent, by consent type or combinations



4. Data Risk Dashboard

IBM Data Risk Manager



GDPR Outcome

iDNA – an Integrated Platform for Business Data Risk. The IBM Data Risk Manager provides visibility to potential risks enabling proactive measures to be applied.

What you don't know *can* hurt you:

- the i-DNA solution provides visibility to potential risks and enables proactive measures to be applied.
- the i-DNA have visibility into critical data.

Visibility into critical data, its residency, controls in place, business usage and potential risks.

… in addition to providing insight into roles and responsibilities across the data lifecycle and ability to view data flows

Prevent, detect and respond to advanced threats:

- Allows early visibility into potential risks to sensitive data
- Identifies specific, high-value business-sensitive data at risk from internal or external threats
- Provides a complete view of sensitive data
- Delivers value and meaning to business executives with a unique, easy-to-understand dashboard
- Enables the right conversations with IT, Security, and LOB teams to improve business processes and mitigate risks