

# 비즈니스를 위한 GDPR (유럽 개인 정보 보호법)

GDPR 준비를 위해 해야 할 일



# Agenda

01

GDPR 개요

02

IBM GDPR  
Framework

03

GDPR 준비 및  
실행을 위한  
솔루션



**\$7.8B**

is how much Global 500 companies will spend on GDPR compliance

Financial Times, "Companies face high cost to meet new EU data protection rules"

# Purpose of the new Regulation\*

## 통합된 데이터 보호 규정 제정

- 1995 년 이전의 EU 데이터 보호와 달리 GDPR은 특정 국가의 정부가 추가로 시행 할 수 있는 법률을 통과시킬 것을 요구하지 않습니다. EU 회원국과 자발적으로 EU 법에 따르는 국가에 적용됩니다.
- 국제적 비즈니스를 위한 규제 환경을 단순화하기위한 것입니다.

## EU 데이터 주체에 대한 데이터 보호 수준을 향상

- GDPR은 개인에게 개인 데이터를 보다 잘 통제하도록 설계되었습니다.

## 기존 및 새로운 기술에 맞게 규제를 현대화

- 예: EU 외부로의 데이터 이전 옵션 증가



\*Per the stated goals from the European Parliament

# GDPR에 대해 알아야 할 6 가지 주요 사항

1

## GLOBAL IMPACT

EU 데이터 주체의 개인 데이터를 처리하는 모든 조직

2

## DATA SUBJECT RIGHTS

중요한 개선 사항으로 인해 데이터 주체의 통제 권한 강화

3

## 전체 매출의 최대 4 %까지 또는 €20M

규정 위반에 따른 손실 비용, 큰 금액을 적용

4

## PRIVACY (AND SECURITY) BY DESIGN

새로운 제품, 시스템 및 서비스에 기본적으로 포함되어야 함.

5

## 72-HOUR BREACH NOTIFICATION

데이터 유출이 발생할 경우 72 시간 이내에 규제 당국에 통보해야 합니다.

6

## TOMs (TECHNICAL AND ORGANIZATIONAL MEASURES)

식별된 위험에 대응하기 위해 구현해야 하는 조치

# GDPR 용어 이해

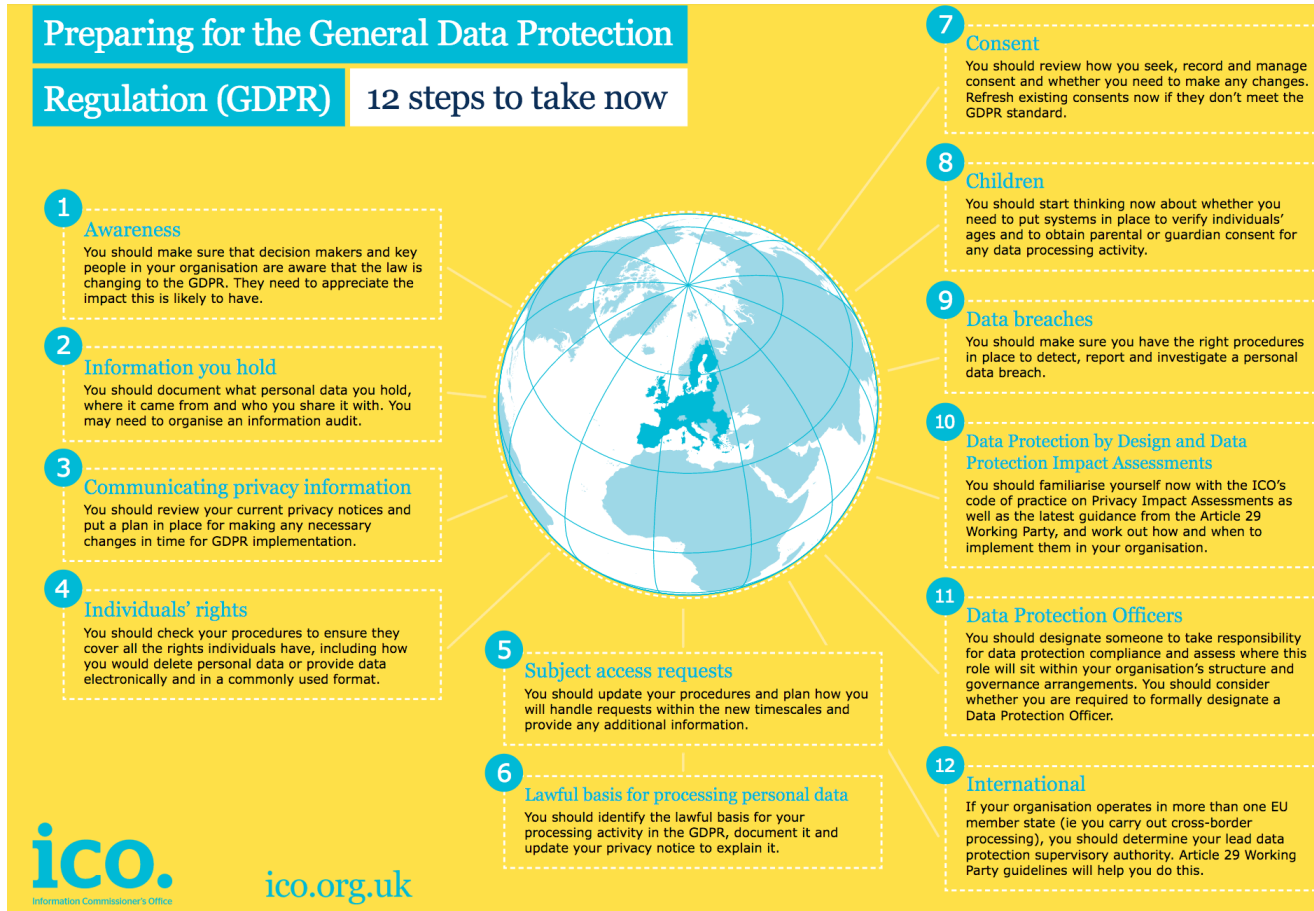
- **Data Subject** - 개인 데이터가 컨트롤러 또는 프로세서에 의해 처리되는 자연인
- **Data controller** - 개인 데이터 또는 개인 정보가 처리되는 방식 및 목적을 결정하는 개인이나 단체
- **Data processor** - 데이터 컨트롤러를 대신하여 데이터를 처리하는 사람 또는 조직 (데이터 컨트롤러는 제외)
- **Data processing** - 수집부터 삭제까지 전체 라이프사이클 동안의 개인 데이터 처리는 "처리 중"으로 간주됩니다. 원격 액세스조차도 "처리 중"으로 간주됩니다.
- **Personal Data** - 식별되거나 식별 가능한 자연인 ('데이터 주체')과 관련된 모든 정보. 이 정의는 이름, 식별 번호, 위치 데이터 또는 온라인 식별자와 같은 개인 데이터를 구성하는 광범위한 개인 식별자를 포함하며, 기술의 변화와 조직이 사람들에 관한 정보를 수집하는 방식을 반영합니다.
- **Sensitive Personal Data** - 인종 또는 민족, 정치적 견해, 종교적 또는 철학적 신념, 노동 조합 회원, 유전자 데이터, 생체 인식 데이터, 건강관련 데이터, 자연인의 성 생활 또는 성적 취향에 관한 데이터.

GDPR은 '컨트롤러'와 '프로세서'에 적용됩니다.

GDPR은 법 집행 기관의 지시에 따른 처리, 국가 보안 목적의 처리 및 개인 / 가정 활동을 위해 개인이 수행하는 처리에는 적용되지 않습니다.

# Guide to the General Data Protection Regulation (GDPR) by ICO

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/introduction/>



# 25%

의 보안 지출은 2019 년까지  
EU 데이터 보호 규정 및 개인  
정보 보호 문제에 의해 주도  
될 것입니다

Source: IDC





# Privacy vs. security: What's the difference?

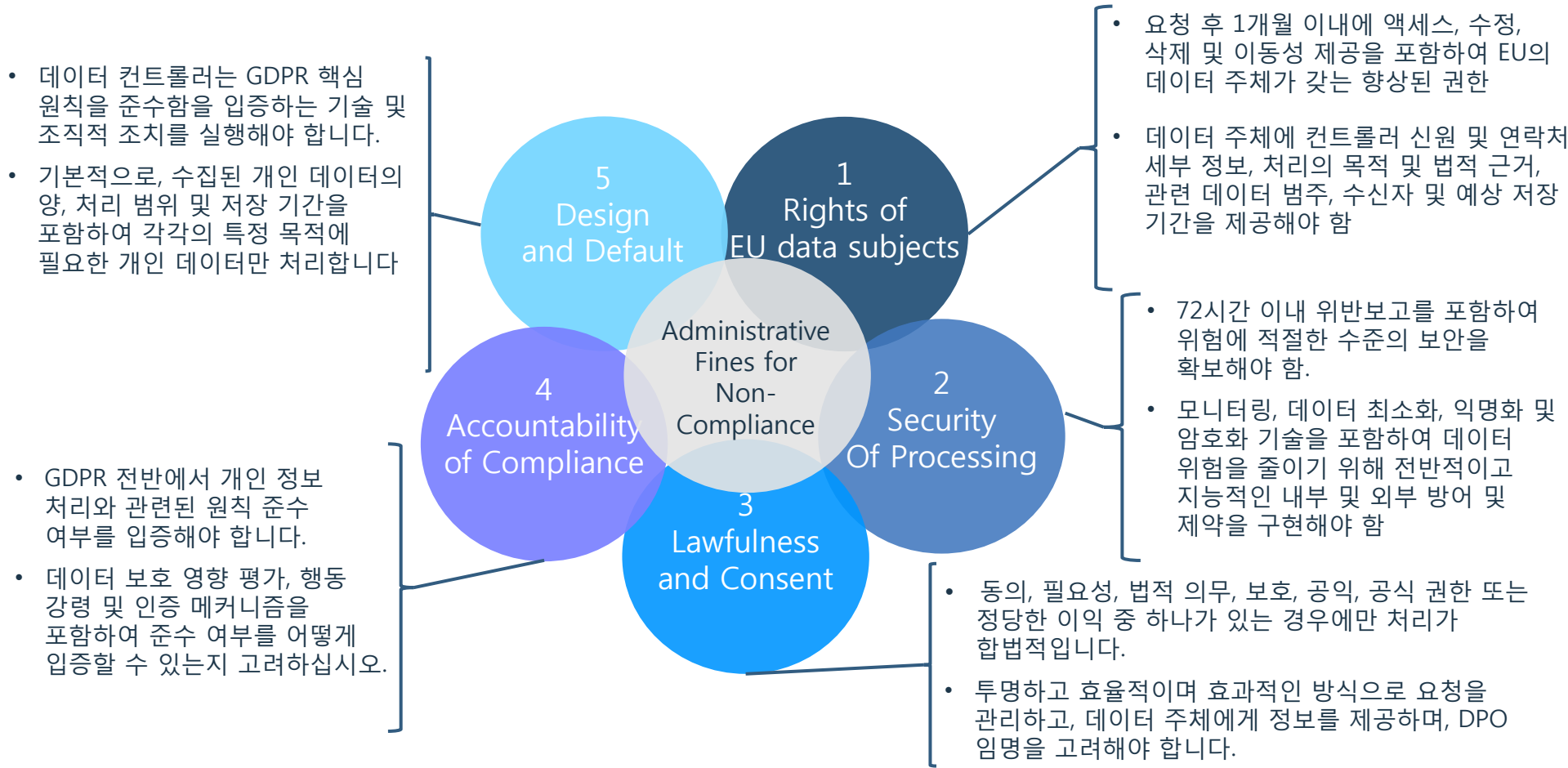
GDPR은 개인 정보 보호와 보안 문제를 모두 다룹니다. 그러나 때로는 이 둘의 차이를 이해하는 것이 어려울 수 있기 때문에 여기에 대해 생각하는 간단한 방법이 있습니다:

- **개인 정보 보호(Privacy)**는 정보의 사용에 관한 것으로, 수집되는 데이터 및 데이터의 사용 방법을 지시하는 정책 및 관행에 관한 것입니다.
- **보안(Security)**은 데이터를 통제하고 보호하는 방법에 관한 것입니다.



# 주요 임무, 의무 및 제재

GDPR 의무를 이해하는데 있어 조직이 알아야 할 다섯 가지 주요 개념이 있습니다:



# GDPR is all About the EU data subject...

"내 데이터를 사용할 대상을  
쉽게 이해하고, 쉬운 선호도  
설정

"나에 대해서 어떤 정보를  
가지고 있으며 무엇을  
위해 사용합니까?

"이 데이터를 다른  
국가로 이전 또는  
처리하고 싶습니다.



"당신이 나를 잊으면  
좋겠습니다.

"내 데이터를 수정하고  
내 데이터를 다른  
서비스제공자에게  
가져가고 싶습니다.

"내 데이터가  
유출 됐는지  
알려주세요.

# GDPR에 대비한 기업들의 준비



The screenshot shows the top navigation bar of the Computerworld website with the logo 'COMPUTERWORLD FROM IDG' and links for 'INSIDER', 'Sign In', and 'Register'. Below the navigation is the author's profile for 'APPLE HOLIC' by Jonny Evans, dated APR 13, 2018 8:07 AM PT. The article is categorized as a 'FEATURE' and has the title 'Everything you need to know about Apple's GDPR privacy upgrade'. The main text states: 'Included in Apple's update to comply with the EU's GDPR, customers will be able to download all the information Apple keeps about them.'

## What is GDPR?

The GDPR rules are designed to bring existing data protection laws into the 21st century. They give individuals the right to see what information companies hold about them, oblige business to handle data more responsibly, and put a new set of fines and regulations in place.

## **GDPR also means Apple will give you more control**

Apple also intends to make it much easier for its customers to control their data. That means we'll be able to:

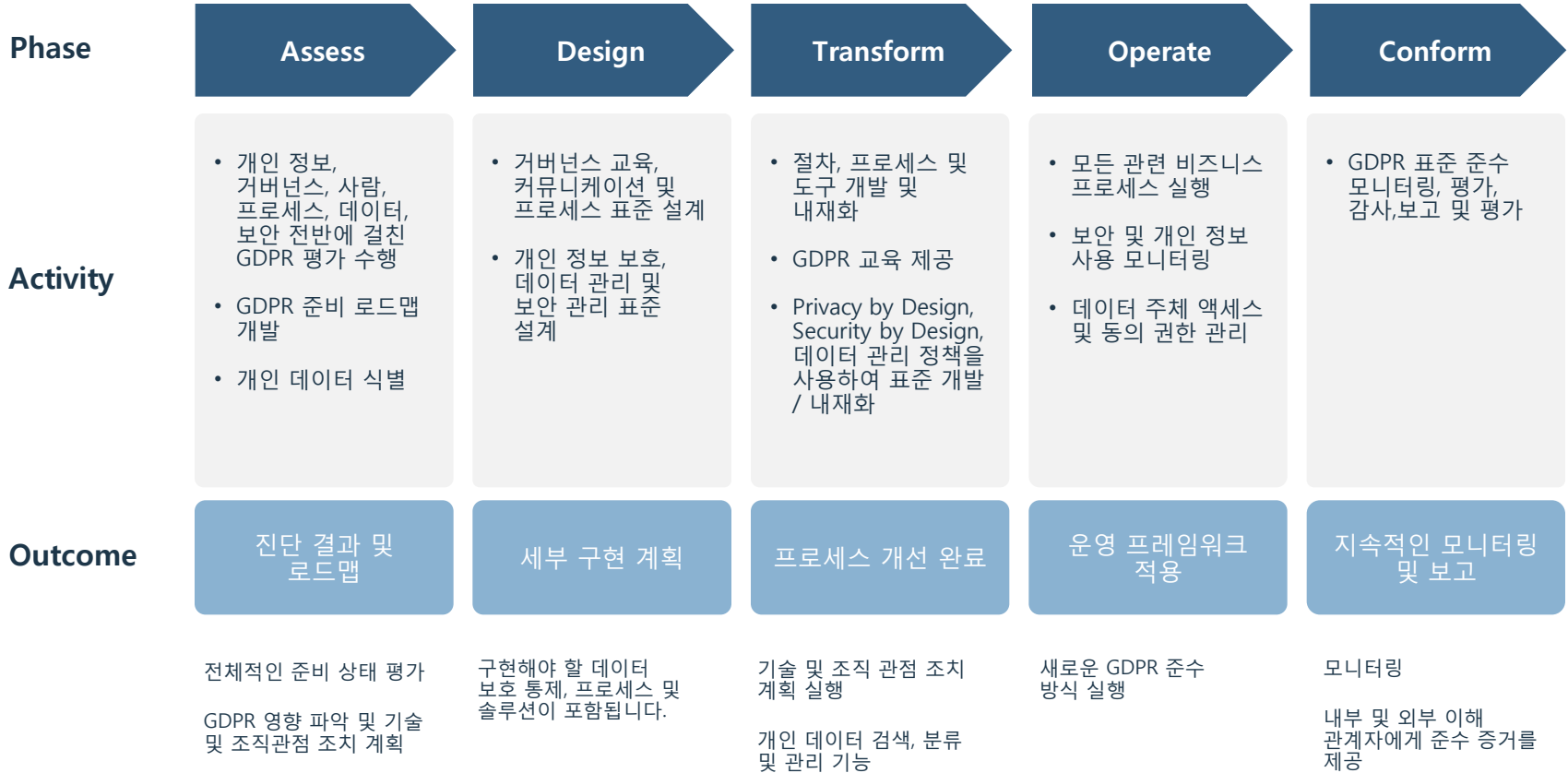
- Get a copy of our data
- Correct our data
- Temporarily deactivate our accounts
- Delete our entire Apple ID



# IBM GDPR Framework



# IBM GDPR Framework



# GDPR 대응을 위한 IBM Security 솔루션

- **GDPR Assessment:** GDPR Readiness Assessment
- **리스크 대시보드:** Critical Data Protection Program + Data Risk Manager
- **개인 데이터 검색 / 분류:** Guardium with GDPR Accelerator, Data Risk Manager
- **데이터 보호 영향 평가, 액세스 리스크:** Guardium Vulnerability Assessment, AppScan Application Security, Identity Governance and Intelligence
- **감사 추적, 데이터 주체 권한 추적 및 생성:** Guardium w/ GDPR Accelerator
- **암호화:** Guardium Data Encryption, Guardium Multicloud Encryption, IBM Security Key Lifecycle Management
- **사건 대응, 위반 통지:** Resilient Incident Response Platform



# GDPR 구현 단계에 따른 IBM Security 솔루션

- GDPR 데이터 검색 및 분류 - **Guardium GDPR Accelerator**
- 액세스 리스크 식별 - **Identity Governance and Intelligence**

## 추가 사항:

- 데이터 라이프사이클 관리
- 데이터 주체 품질 관리
- 위험 및 규정 준수 관리

- GDPR 데이터 액세스 이력 기록
- 데이터 프로세서 / 컨트롤러 거버넌스 실행
- **Guardium GDPR Accelerator**
- 침해 대응 및 관리
- **Resilient Incident Response**



- 보안 참조 아키텍처 수립
- 위험 측정 및 지표 정의
- **Guardium Data Protection, Identity Governance, Guardium Data Encryption**

- 개인 정보 보호 강화 통제 구현
- **Guardium Data Encryption**
- 보안 통제 구현 **Guardium Data Protection, Identity Governance**

- 개인 데이터 액세스 모니터링
- 데이터 액세스 관리 및 인증
- 데이터 사고 대응 및 조사
- 위험 모니터링, 탐지, 대응 및 완화
- **Guardium GDPR Accelerator, Identity Governance and Intelligence, QRadar, Resilient Incident Response**





# GDPR 준비 및 실행을 위한 솔루션



# GDPR이 비즈니스에 미치는 영향을 어떻게 측정합니까?

SOLUTION

## GDPR Readiness Assessment

### 주요 특징

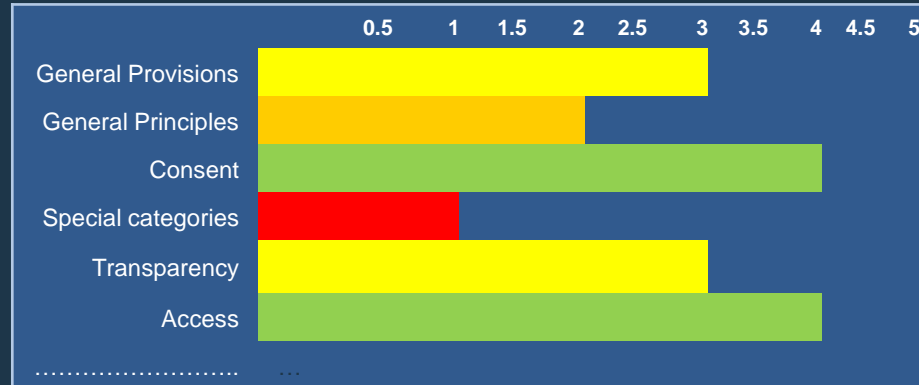
- GDPR의 영향을 받는 사업 영역을 식별
- 새로운 요구 사항에 대해 현 실행 내용 평가
- 프로세스 개발, 모범 사례 및 조직의 요구에 중점을 두고 프로젝트 진행
- 산출물에는 성숙도 모델, 갭 분석 및 이행 계획이 포함됨
- 다음 단계에 적합한 제품 및 서비스를 제안

## GDPR Readiness Assessment Maturity Model

### Key

Level 5 – Optimizing	프로세스는 지속적으로 평가되며, 프로세스 개선에 중점을 둡니다.
Level 4 – Managed	프로세스가 측정되고 제어됩니다. 성숙된 프로세스가 실행되고 있습니다.
Level 3 – Defined	조직의 프로세스가 식별되었습니다. 종종 사전 대책을 세웁니다.
Level 2 – Repeatable	최소한의 활동이 수행되고 있습니다. 특정 상황에 대응합니다.
Level 1 – Initial	평가된 요구 사항에 대한 어떠한 활동도 수행되지 않고 있습니다.

### Maturity by Area (partial example of assessment results)



ASSESS

DESIGN

TRANSFORM

OPERATE

CONFORM

# 개인 데이터를 찾고 액세스 권한을 추적하려면 어떻게 합니까?

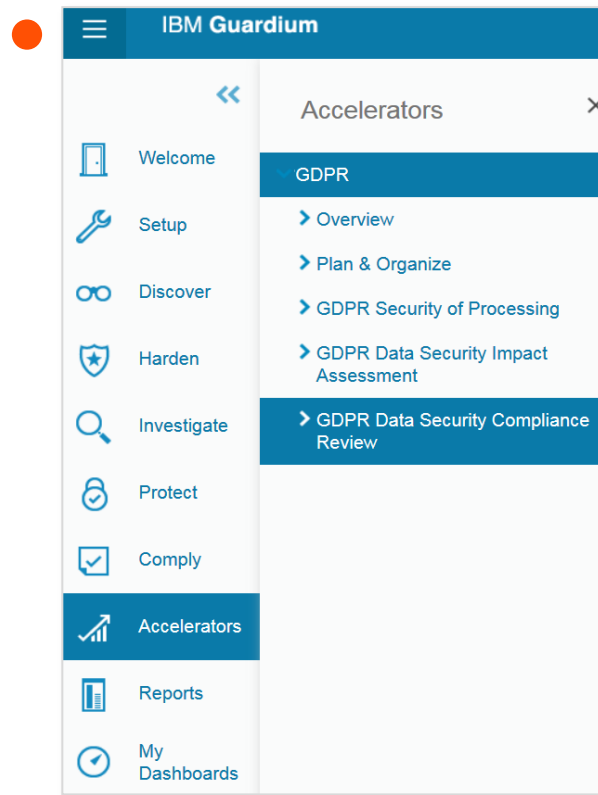
SOLUTION

## IBM Security Guardium® GDPR Accelerator

### 주요 특징

- 개인 데이터에 대한 데이터 검색 및 분류
- 데이터 주체 요청 및 개인 데이터 액세스를 포함한 GDPR 개인 데이터의 감사 및 모니터링 보고서
- GDPR 개인 데이터를 위한 사전 정의 된 정책 및 그룹
- 감사자, 컨트롤러 및 데이터 프라이버시 담당자를 위한 컴플라이언스 워크플로우 및 감사 프로세스 빌더
- Guardium Data Protection 제품의 일부로 포함되어 제공됨

GDPR 특정 의무사항과 관련된 미리 정의 된 지식 집합



ASSESS

DESIGN

TRANSFORM

OPERATE

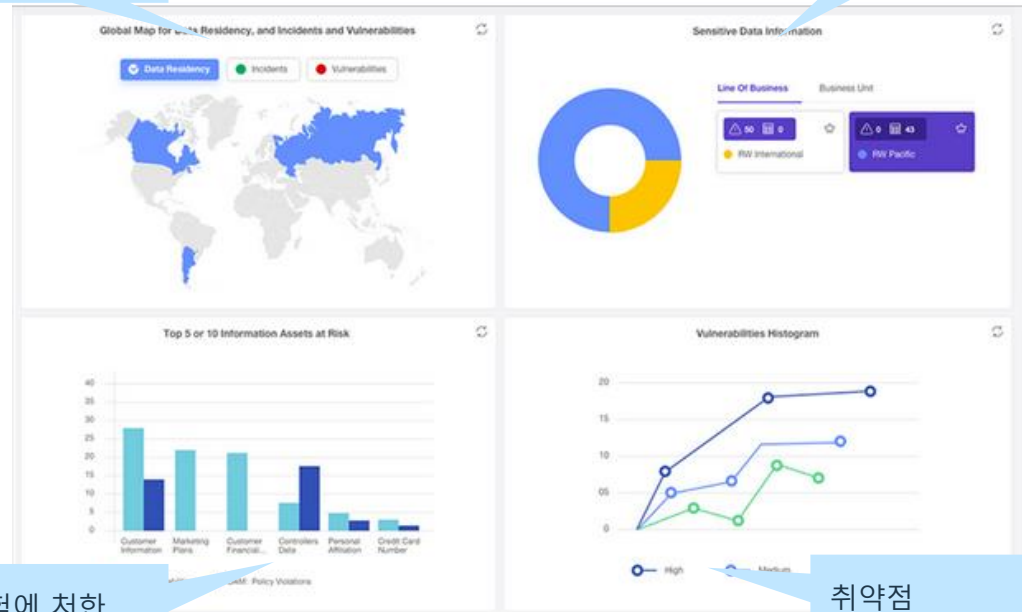
CONFORM

# 위험이 어디에 있는지 어떻게 알 수 있습니까?

데이터 위험 관리 센터는 데이터 관련 비즈니스 위험을 파악하고 해결을 지원합니다.

데이터 위치 및  
취약점 매핑

민감한 데이터  
정보 시각화



위험에 처한  
주요 정보 자산

취약점  
히스토그램

SOLUTION

## IBM Data Risk Manager

### 주요 특징

- 내부 및 외부의 위협으로부터 위험이 있는 가치가 높고 비즈니스에 민감한 정보 자산을 식별
- 애플리케이션 및 비즈니스 프로세스 모두에 대해 데이터 프로세서 및 데이터 컨트롤러에 대한 가시성 확보
- 데이터 노출을 시각화 하여 경영진이 IT, 보안 및 비즈니스 라인과 대화 할 수 있도록 지원
- IBM Security Guardium® GDPR Accelerator와의 통합 지원

ASSESS

DESIGN

TRANSFORM

OPERATE

CONFORM

# 누가 개인 데이터에 대한 액세스 권한이 있으며 리스크가 있습니까?

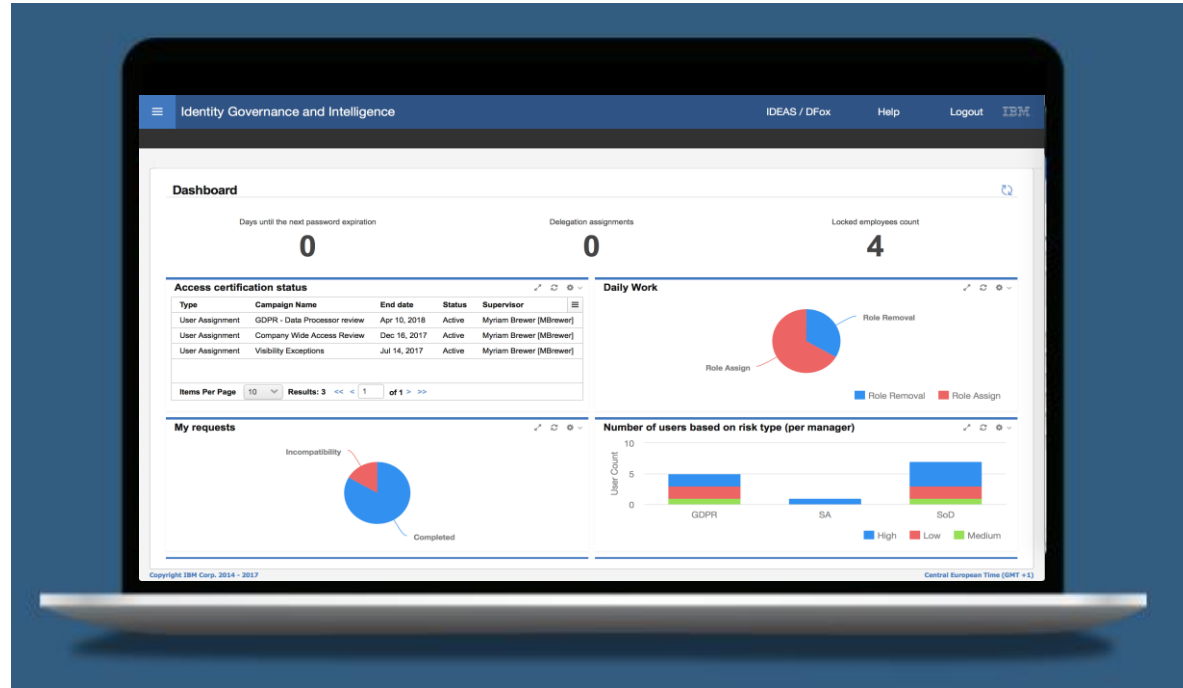
애플리케이션 액세스 및 개인 정보에 대한 액세스 위험을 식별하고 완화합니다. 액세스 및 ID 라이프사이클 프로세스 자동화

SOLUTION

## IBM Security Identity Governance and Intelligence

### 주요 특징

- ID 및 액세스 라이프 사이클 관리
- 엔터프라이즈 및 클라우드 애플리케이션의 컴플라이언스 통제위반 표시
- 고급 분석 및 리스크 스코어링을 통해 롤 및 권한 최적화
- 데이터 처리자에 의한 개인 정보 액세스 파악 및 분류
- 애플리케이션 및 데이터 액세스 전반에 걸쳐 GDPR 관련 통제 및 보고서를 제공



ASSESS

DESIGN

TRANSFORM

OPERATE

CONFORM

# GDPR 제 32 조의 보안 처리 방법을 어떻게 구현합니까?

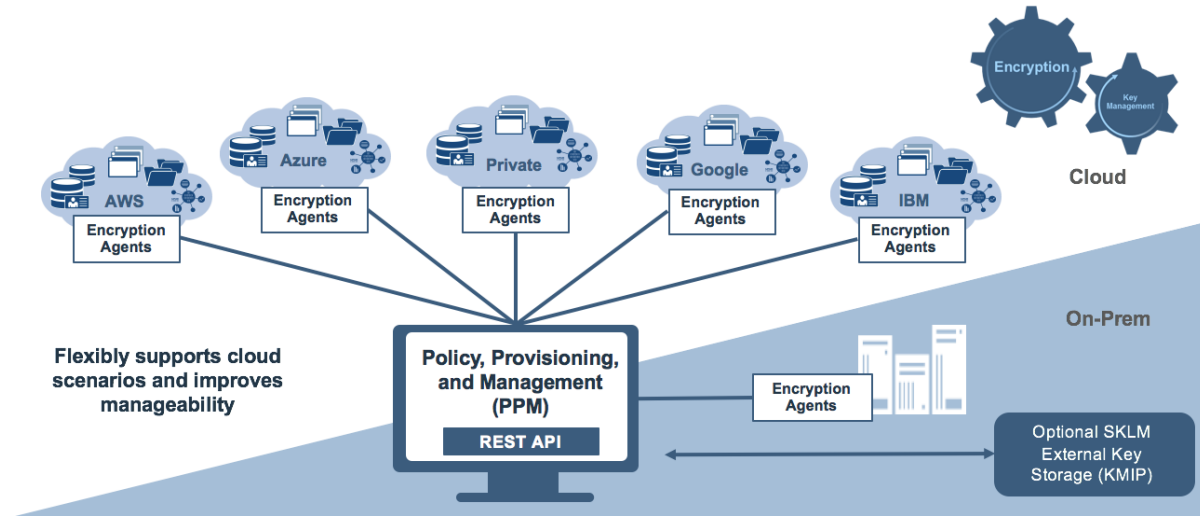
SOLUTION

## IBM Multi-Cloud Data Encryption

### 주요 특징

- 프로세스 기반 액세스 제어 및 간소화된 관리 인터페이스를 통한 정책 집행과 직무 분리
- 암호화 키 순환을 이용한 고급 암호화 분할 기술
- 액세스 제어를 유지하면서 파일 및 볼륨 데이터 암호화, 자동 HA Failover 지원
- 풍부한 REST API 지원
- 복잡한 암호화 환경에서 보안이 강화된 키 관리 기능을 제공하는 IBM Security Key Lifecycle Manager 통합방안 제공

On-prem, 단일 클라우드, 멀티 클라우드, 하이브리드 환경 등 데이터의 위치에 관계없이, 파일 및 볼륨 암호화 기능을 통하여 오용으로 부터 데이터 보호



ASSESS

DESIGN

TRANSFORM

OPERATE

CONFORM

# 72 시간 이내 위반 통지 요구 사항을 어떻게 충족시킬 수 있습니까?

## SOLUTION

# IBM Resilient® Incident Response Platform

## 주요 특징

- 인시던트를 보다 신속하게 분석, 대응, 해결 및 위험을 완화하는 방안을 제공
- 신속하고 효과적인 대응이 이루어지도록 분석가를 안내하는 모범 사례 기반의 사고 대응 계획을 제공
- 기존 IT 및 보안 기술을 사고 대응 관리를 위한 단일 허브에 통합
- 단순화된 워크 플로우 구성 및 프로세스 자동화 가능

Resilient 사고 대응 플랫폼에 내장된 GDPR 관련 도구를 사용하여 GDPR에 대한 준비 및 실행



## • GDPR Preparatory Guide

잘 정의되고 문서화된 프로세스를 통해 GDPR 준비 및 대응을 지원

## GDPR Simulation

보안 팀은 GDPR에 따른 사건에 대응하기 위해 향후 취해야 할 조치를 훈련 할 수 있습니다.

## • GDPR-Enhanced Privacy Module

보안팀은 GDPR 관련 지침 및 IRP에 포함된 법률에 관한 업데이트된 데이터베이스에 액세스 할 수 있습니다.

ASSESS

DESIGN

TRANSFORM

OPERATE

CONFORM

## GDPR 대응을 위한 실행 계획



- I. GDPR Readiness Assessment
- II. Personal Data Mapping & Discovery
- III. Build a Remediation Plan



# Interactive assessment tool: [ibm.biz/GDPR-Ready](https://ibm.biz/GDPR-Ready)



IBM Security

Share

## Is your business ready for GDPR?

The EU General Data Protection Regulation (GDPR) has a tremendous impact on the way organizations handle data. Use our **Guide to GDPR Readiness** to determine the steps your company can take surrounding GDPR.

[I'm ready to get started!](#)

## About GDPR

GDPR aims to harmonize data protection across all 28 EU member states and businesses within the regions. If your organization is active across the EU, understanding and activating initiatives related to GDPR is necessary in order to continue conducting business.

[Learn More](#)



## Request a Consultation

IBM is positioned to help you develop strategies to address all the challenges surrounding GDPR. Request a consultation with IBM to learn more about our phased program engagement points and cognitive capabilities to help accelerate your GDPR journey.




[Contact Us](#)





# THANK YOU

## FOLLOW US ON:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.