Zoom In

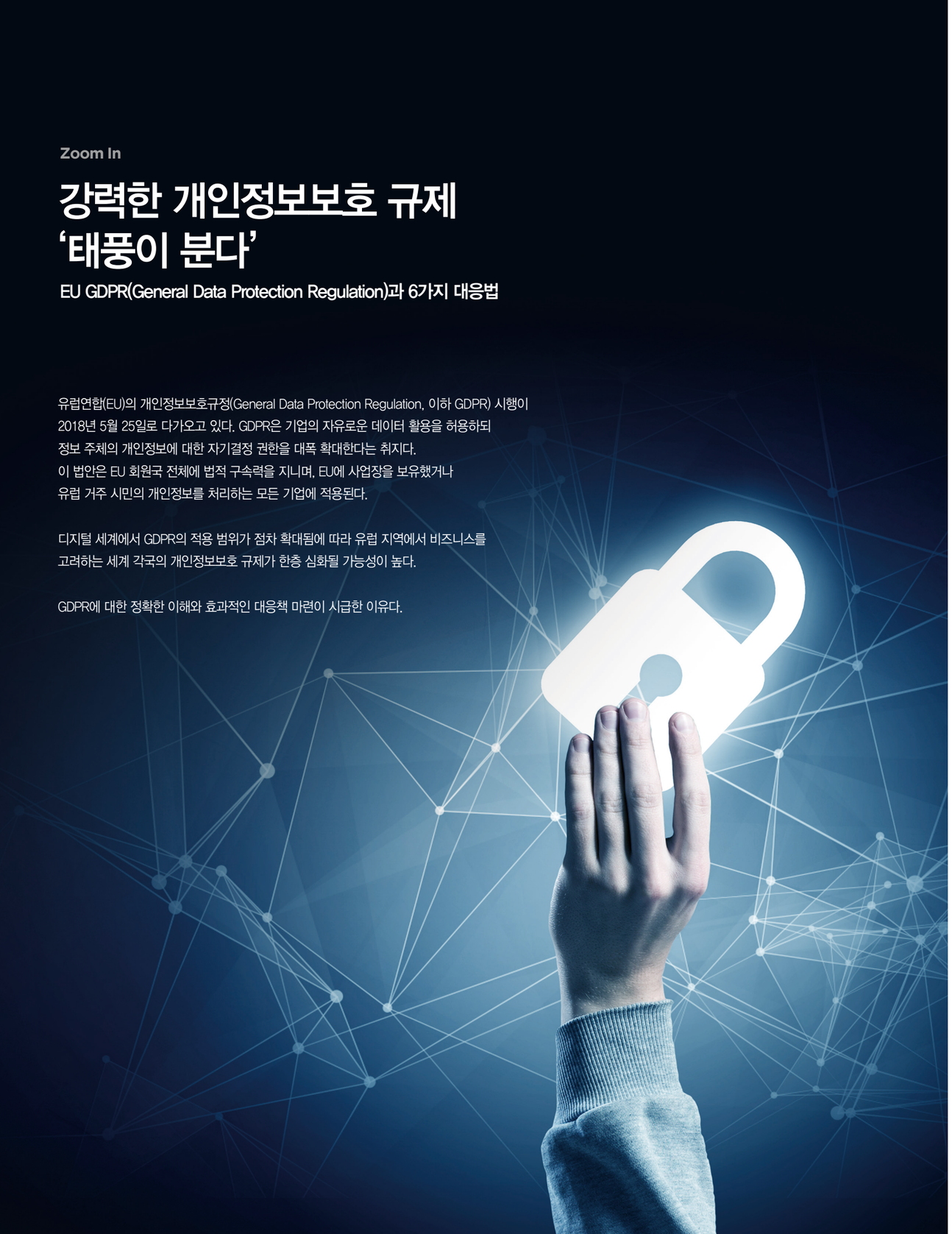
강력한 개인정보보호 규제 '태풍이 분다'

EU GDPR(General Data Protection Regulation)과 6가지 대응법

유럽연합(EU)의 개인정보보호규정(General Data Protection Regulation, 이하 GDPR) 시행이 2018년 5월 25일로 다가오고 있다. GDPR은 기업의 자유로운 데이터 활용을 허용하되 정보 주체의 개인정보에 대한 자기결정 권한을 대폭 확대한다는 취지다. 이 법안은 EU 회원국 전체에 법적 구속력을 지니며, EU에 사업장을 보유했거나 유럽 거주 시민의 개인정보를 처리하는 모든 기업에 적용된다.

디지털 세계에서 GDPR의 적용 범위가 점차 확대됨에 따라 유럽 지역에서 비즈니스를 고려하는 세계 각국의 개인정보보호 규제가 한층 심화될 가능성이 높다.

GDPR에 대한 정확한 이해와 효과적인 대응책 마련이 시급한 이유다.



GDPR은 EU 시민들을 대상으로 비즈니스를 하거나, EU 거주 정보 주체에 대한 개인식별정보(Personally Identifiable Information, 이하 PII)[1]를 수집해 사용하거나 보유하는 모든 기업들에게 적용되는 법안이다. 미국 기업들을 대상으로 하는 사베인 옥슬리(Sarbanes-Oxley, SOX)[2], GLBA[3], HIPAA[4] 등 보다 훨씬 더 큰 영향을 미칠 것으로 분석된다. 개인 정보에 대한 수많은 규제와 변화 요인에 대응하기 위해 기업들은 자율적인 내부 규제 강화를 통해 비즈니스 연속성 확보하고자 IT 컴플라이언스(Compliance)에 대한 중요성을 인지하기 시작했다. IT 컴플라이언스란 기업의 투명성을 강화하고 리스크를 관리하기 위해 각종 규제 법안을 만족할 수 있도록 IT 관점에서 기업 내 시스템을 정비하는 의무 활동 전반을 가리킨다.

GDPR의 요구사항

GDPR은 새롭게 적용해야 하는 내용을 담은 99개의 조항으로 이루어진 방대한 규모의 법령이다. 데이터 주체가 되는 EU 거주인을 식별하기 위한 모든 정보(위치 정보, IP 주소, 차량 번호판, 인종 및 의료정보 등)를 아우르는 새로운 유형의 PII를 세세하게 다루고 있으며, 이는 기업에서 상대하는 모든 고객과 방문자, 뉴스레터 구독자, 앱 사용자, 임직원 등 모든 사람들에게 해당된다.

컴플라이언스를 준수하기 위해서는 다양한 프로세스와 시스템을 대대적으로 변화시켜야 하며, 대표적인 내용들만 나열해 보면 아래와 같다.

- 데이터 수집 동의 항목을 명확하고 구체적으로 기술해야 하며, 특히 어떤 데이터가 어떻게 사용되고 얼마나 보관되는지를 명시해야 한다. 30페이지 분량의 법률 용어가 가득한 텍스트 하단에 체크박스만 넣는 형태는 허용되지 않으며, 각각의 데이터 사용 목적에 대해 별도의 동의를 얻어야 한다.
- 개별적인 데이터 주체에 대한 처리 요청이 가능해야 한다. 동의 철회, 정보 삭제(잊혀질 권리), 데이터 복제본 제공, 타 기관으로의 데이터 이동, 오류 정보에 대한 수정 등이 '시의 적절하게' 이루어져야 한다.
- 주기적인 프라이버시 영향 평가를 수행함으로써 데이터 거버넌스 규정에 포함되지 않았던 새로운 시스템 및 데이터 소스를 점검해야 한다.
- 데이터 침해 사고 발생 시 72시간 이내에 각 지역의 데이터 보호 당국 및 피해 당사자에게 사고 내용이 고지돼야 한다.
- PII를 공유하는 DPA(EU 개인정보감독기구)와 모든 정보관리자에 대한 감사 자료를 제출해야 한다.
- 마케팅 에이전시 및 로열티 프로그램 관리자 등 PII를 공유하는 제3의 기관도 모두 GDPR을 완벽하게 준수할 수 있도록 관리해야 한다.
- 독립적인 권한을 가진 데이터 보호 책임자(Data Protection Officer)를 고용하거나 임명해 전체적인 데이터 거버넌스 및 GDPR 규정 준수 업무를 담당하도록 해야 한다.

결국 GDPR의 핵심 주제는 모든 제품과 서비스에 '프라이버시 중심 설계(Privacy by Design)'를 적용하도록 하는 것이다.

발등의 불 'GDPR'

GDPR 위반 범칙금도 2천만 유로(한화 270억 원) 혹은 글로벌 매출의 2% 중 큰 금액으로 부과되며, 매출 기준은 모회사 혹은 자회사의 매출을 모두 포함한 금액이다. 데이터 수집 주체인 데이터 취급자라면, 제3의 데이터 처리자가 위반한 내용에 대해서도 범칙금을 물어야 한다. 여기에 국경 간 데이터 이동에 대해서도 고려해야 한다.

1) PII(Personally Identifiable Information): 개인 식별 정보. 이름, 주소, 이메일 주소, 신용카드번호, 주민등록번호, 인터넷 주소 등 개인을 직접 식별하거나 유추해 알 수 있는 모든 정보를 말한다.
2) 사베인-옥슬리 법(Sarbanes-Oxley Act): 기업 관리자가 금융 데이터의 잘못된 해석에 대한 개인적인 책임을 지도록 규정한다. 이로 인해 많은 기업들이 회계관리, 내부통제시스템 도입 및 경영인증시스템을 구축했다.
3) GLBA(Gramm-Leach-Bliley Act): 은행, 증권, 보험 등 모든 금융 업무를 하나의 회사가 운영할 수 있도록 허용한 법(일명 GLB법)에 따라 모든 금융 기관은 고객의 개인정보를 안전하게 보호할 수 있는 조치를 취하도록 의무화한다.
4) HIPAA(Health Insurance Portability and Accountability Act): 모든 의료 기관은 환자 정보를 6년간 보호하도록 의무화한다.

GDPR에서 법적으로 금지된 것은 아니지만 프라이버시 데이터 조약이 제공되는 곳으로만 데이터를 이동할 수 있도록 제한하고 있다. 예를 들어 미국과 유럽의 경우 이전의 세이프 하버(Safe Harbor)[5] 혹은 현재의 프라이버시 실드(Privacy Shield)[6]의 보호를 받는 곳으로만 데이터를 이동시킬 수 있다. 하지만 사용 중인 클라우드 서비스의 데이터가 아마존, 구글, 마이크로소프트 등 서비스 제공업체의 어떤 데이터센터에 저장돼 있는지 알고 있는 사용자는 얼마나 될지 의문이다.

일각에서는 GDPR 범칙금이 재정 악화를 겪고 있는 EU의 새로운 수익원으로 사용될 것이라는 냉소가 있기도 하지만 2018년 5월 25일 이후, 높은 범칙금이 부과되는 사례들을 목격할 수 있을 것이다. 그리고 이러한 범칙금을 내는 기업들 대부분은 아주 많은 유럽인들을 고용한 것은 아니지만 전세계 시장에서 비즈니스를 하고 있는 다국적 기업들이 될 것이다. 만약 유럽 기업들이 이 제도로 인해 파산하거나 직원을 해고해야 할 지경이라면 대단히 큰 반감을 사겠지만, 실상은 미국 혹은 그 이외의 지역에 본사를 둔 기업들에게는 문제가 여간 큰 것이 아니다.

GDPR 준비 '우왕좌왕'

GDPR을 기업에서는 어떻게 대처해야 할까? GDPR 준수와 임시 대처, 그리고 아웃소싱 등 방안을 놓고 혼란스러워할 것이 분명하다. 전 세계 많은 기업에서 이미 활발한 논의가 이루어지고 있으며, 법안이 시행될 2018년에는 더 적극적으로 상황에 대처하기 위해 컴플라이언스 비용을 따져보고, EU 시장의 잠재 이윤에 따라 해당 지역에 대한 비즈니스 존속을 고민하는 사례가 늘어날 전망이다. 실제로 보안 서비스 제공업체 SureCloud가 최근 실시한 조사에서는 '미국 기업의 상당수가 GDPR에 대비하는 것보다 유럽 비즈니스를 축소하거나 중단하는 것을 선택할 것' 이라는 결과가 나오기도 했다.

GDPR 시행에 대응하기 위해 국내에서도 대책 마련에 나섰다. 행정자치부는 한국인터넷진흥원(KISA)과 함께 지난 4월부터 '우리 기업을 위한 유럽개인정보보호법 안내서' 를 발간하고, '유럽 개인정보보호법 설명회' 를 개최하면서 GDPR에 대한 인식 확산과 대응에 많은 노력을 기울이고 있다. 하지만 정보 주체 중심의 실질적인 보호체계를 요구하는 GDPR은 한국의 개인정보보호법과 많은 차이가 있어 준비에 난항을 겪고 있다. 산업계에서도 일부 대기업을 제외하고는 GDPR에 대해 적극적으로 준비하는 움직임을 보이지 않고 있다.

시장조사기관 밴슨본(Vanson Bourne)이 올해 발표한 조사에서 국내 기업 GDPR 준비 현황을 살펴보면, 국내 응답자의 61%는 내년 5월 내에 GDPR 규정 준수를 위한 대비를 마치지 못할 것이라고 답했다. 응답자의 40%는 실시간으로 DB를 모니터링하는 툴이 없어 관리가 불가능하다고 답했으며, 29%는 관련 데이터를 정확하게 식별하거나 위치 파악이 어렵다고 우려를 표했다. 기업의 책임은 커졌지만 GDPR에 대한 인식과 기술적 준비도 갖춰지지 않은 상황이다.

GDPR 준수 위한 6가지 대응법

GDPR의 핵심 요건에 대응하기 위해서는 종합적인 데이터 관리 시스템의 기반을 마련해야 한다. 데이터 관리 전문 회사들은 GDPR을 비롯해 점차 강화되는 각종 컴플라이언스 이슈 대응에 도움을 줄 수 있도록 다양한 솔루션을 제시하고 있다. 효성인포메이션시스템(이하 HIS)의 합작사인 Hitachi Vantara(히타치 밴타라)는 오브젝트 스토리지인 HCP(Hitachi Content Platform)와 보관된 데이터로부터 빠르게 정보를 검색하고 분석까지 수행하는 HCI(Hitachi Content Intelligence)를 제안한다.

기업들이 충족시켜야 하는 GDPR의 핵심 요건과 이를 준수하는 데 도움을 줄 수 있는 방안을 데이터 관리 차원에서 여섯 가지로 나눠 알아보자.

1) 세이프하버(Safe Harbor): 의료분야에서 많이 언급되고 있는 미국의 방식으로 이름, 주소 등 18가지 주요 식별자를 제거하도록 규정하고 있다. 이를 잘 지킬 경우 비식별 조치한 데이터 집합 내에서 한 개인이 재식별될 확률은 0.04%로 추정된다.
2) 프라이버시 실드(Privacy Shield): 미국이 EU와 2016년 도입한 개인정보 국외 이전 협약. 유럽에서 미국으로 데이터를 보낼 때 유럽이 정한 정보보호기준 준수 사실을 스스로 입증해야 하며, 부당하게 정보가 사용될 경우 EU는 미국 법원에 소송을 걸 수 있도록 했다.

01 메타데이터 관리

개인정보를 광범위하게 수집하고 효율적으로 관리할 수 있어야 한다. GDPR이 요구하는 데이터 정확성, 사용자 동의, 보관 기간 문제를 해결하기 위해선 데이터뿐 아니라 그 속성 정보를 담은 메타데이터를 함께 보관해야 한다. 이러한 메타데이터를 생성, 보관, 관리하는 오브젝트 스토리지 기술을 사용하면 검색과 분석이 쉽지 않은 비정형 데이터에 정형성을 부여하게 돼, 데이터베이스 없이도 많은 양의 콘텐츠와 메타데이터를 간편하게 저장하고 효율적으로 활용할 수 있다.

HIS 솔루션 클라우드 오브젝트 스토리지인 HCP는 보안과 안정성이 강화된 엔터프라이즈용 오브젝트 스토리지다. 고품질 메타데이터를 수집해, 데이터의 물리적 위치와 상관없이 강화된 데이터 가시성, 자동화 및 정책 기반 관리를 제공한다. 빌트인된 오브젝트 기반의 메타데이터 시스템은 특히 정형 데이터뿐 아니라 급증하고 있는 비정형 데이터에 대한 검색 및 분석이 용이하도록 지원한다. 메타데이터 분석을 적용해 인텔리전스 기능을 강화했다. 또한 중앙 집중식 관리 기능으로 고객이 자신의 조건에 맞게 퍼블릭 클라우드 스토리지를 통합하는 하이브리드 클라우드 스토리지를 안전하게 통합 적용할 수 있어 민첩성을 향상시키고 비용을 최적화할 수 있게 해준다.

02 검색 및 분석

개인정보를 손쉽고 빠르게 검색할 수 있어야 한다. GDPR은 기업이 보유 중인 정보에 대해 액세스와 가용성을 보장하도록 요구한다. 정보 주체가 자신의 정보 조회를 요청할 경우, 기업은 전 시스템에 걸쳐 사용된 내역을 모두 공개해야 하기 때문에 신속하고 적절하게 응답할 수 있는 스토리지 시스템이 필요하다. 오브젝트 스토리지에서 메타데이터 쿼리 매커니즘, 콘텐츠 검색 및 인덱싱 옵션 기능을 제공하는 솔루션을 사용하면 빠른 검색이 가능하고, 다양한 업계 표준 프로토콜을 통해 저장된 데이터에 액세스할 수 있다.

HIS 솔루션 HCP 포트폴리오는 업계 최초 및 유일의 콘텐츠 인텔리전스 기능을 갖춘 오브젝트 스토리지 포트폴리오로, 여기에 속하는 HCI는 데이터 활용 및 분석을 위한 콘텐츠 인텔리전스 솔루션으로 신속하고 정확한 검색 및 분석 기능을 갖추고 있다. 또한 HCI가 제공하는 인텔리전스 기능은 데이터의 활용에 대한 보고서를 생성함으로써, 새로운 인사이트를 제공하고 데이터 가치를 확대할 수 있다. 유용한 정보를 제공해 컴플라이언스 요건의 충족을 지원할 수 있는 것이다.

03 데이터 보호 및 보안

개인정보의 완벽한 보호와 보안이 가능해야 한다. GDPR은 기업이 개인정보의 보호를 위해 적절한 기술적, 조직적 조치를 취할 것을 요구한다. 홍콩 및 호주를 비롯한 아시아태평양 국가들도 오래 전부터 무단 액세스 방지 조치를 요구해 왔으며, 최근 중국이나 인도는 정보 보안을 위해 기술 차원에서 보다 엄격한 방식을 개발하고 있다.

HIS 솔루션 오브젝트 스토리지는 강력한 접근 관리와 암호화 기능을 제공한다. 지정된 IP 또는 IP 대역을 화이트리스트 또는 블랙리스트 방식으로 지정해 시스템에 대한 접근 정책을 설정할 수 있으며, 데이터의 읽기, 쓰기, 삭제, 검색 등의 권한을 구분해 부여해 데이터를 안전하

HCI의 데이터 관리 기능

조직적인 데이터 관리의 간편화
- 클라우드 환경의 멀티 구조 데이터를 통합해 데이터 연결성 강화
- 데이터 커스터마이징 및 메타데이터 저장을 통한 데이터의 가치 증대

데이터 기반의 의사결정 지원
- 데이터의 형태 및 소스에 무관한 실시간 데이터 접근
- 데이터 분류, 검색, 커스터마이징의 중앙화 지원

비즈니스 트랜스포메이션의 기반 마련
- 오픈코어 기반 클러스터 구조를 통한 엔터프라이즈급 확장성 지원
- 물리적 환경, 가상머신, 클라우드 호스팅 등 다양한 플랫폼에 적용 가능

게 보호한다. 또한 HCP는 모든 데이터 접근 기록을 별도로 보관하며, 이를 향후에도 지속적으로 모니터링할 수 있도록 지원한다. 데이터 암호화 기능을 제공하며, 암호화 키는 내부에 분산 저장되므로 지정된 권한 없이는 데이터를 읽을 수 없고 디스크나 노드 도난 시에도 안전하다.

04 수정 방지 및 복구

개인정보의 무결성과 진본성을 보장할 수 있어야 하며, 보유한 개인정보가 정확하고 변경되지 않았다는 사실을 입증할 수 있어야 한다. 특히 파일 데이터의 경우 파일시스템이나 운영체제 등의 논리적 오류로 인한 파일 손상이 간혹 발생하는 경우가 있는데, 오브젝트 스토리지는 이러한 논리적 데이터 훼손까지도 주기적으로 체크하고 이를 복구하는 기능을 제공해 파일 데이터의 무결성을 보장할 수 있다.

HIS 솔루션 HCP는 실수나 고의로 인한 수정이나 훼손, 삭제로부터 데이터를 안전하게 보호할 수 있다. HCP는 WORM(Write Once Read Many) 기능을 제공해 데이터의 수정을 금지하고 안전하게 파일을 보호한다. 또한 일정 기간 동안 수정되기 전의 파일을 보관하는 버저닝(Versioning) 기능을 이용해 변경되기 직전의 파일로 간편한 복구가 가능하다. 또한 파일마다 고유의 식별ID를 제공하는 암호화 기술인 해시 키(HASH Key)를 생성해 함께 보관하므로, 파일에 대한 진본성과 무결성을 입증하는 데 효과적이다.

05 보존 기간 적용

효과적인 개인정보 보유 및 보존 시스템을 마련해야 한다. GDPR은 보유 기간의 제한을 규정하고 있으며, 이는 엄격한 규제 환경과 민감한 데이터의 증가로 모든 비즈니스에서 요구되는 사항이다.

HIS 솔루션 HCP는 데이터의 보존기간을 설정할 수 있는 기능을 제공하므로, 기업이 데이터의 중요도와 활용 가치에 따라 보존기간에 대한 정책을 유연하게 적용할 수 있도록 지원한다. 컴플라이언스 모드의 경우 강력한 데이터 보호를 위해 적용하며, 보존주기 내에서는 어떠한 파일에 대한 삭제 시도도 불가능하다. 엔터프라이즈 모드에서는 보다 유연한 정책 적용을 통해 특별 권한을 가진 사용자에 의한 삭제나 보존기간 변경 등이 제한적으로 허용된다.

06 잊혀질 권리 보장

개인정보의 완벽한 삭제가 가능해야 한다. 정보 주체가 정보 삭제를 요청하면 기업은 모든 시스템에서 정보를 영구적으로 삭제하고 이를 입증할 수 있어야 한다.

HIS 솔루션 전용 검색 솔루션인 HCI의 경우, 오브젝트 스토리지에 보관된 개인정보가 포함된 파일들을 빠르게 찾을 수 있다. 또한 HCP는 이를 삭제 시 파일 블록 전체에 특정 값과 무작위 값을 여러 번 덮어쓰기 하는 방식으로 재처리해, 미국 방성이나 국정원 기준을 준수하는 완벽한 논리적 디지털 파쇄를 구현할 수 있다. 또한 데이터의 수명 주기 전반에 걸친 모니터링을 통해 일반적 삭제나 권한 삭제, 자동 삭제 등 데이터 삭제 작업이 모두 기록되어 관리된다.

HCP 포트폴리오의 데이터 보호 및 관리 기능

강력한 보호 정책

- 저장 파일에 대한 강력한 보호(수정 금지, 보존기간 내 삭제 방지)
- 파일 수정 및 변경 기능을 통해 잘못된 변경 혹은 삭제 시 복원
- HW 보호 기법인 RAID와 클라우드 환경에서의 SW 보호 기법 동시 적용
- 클라우드 및 기업 환경에서 필요한 접근 제어 및 권한 중심의 계정 관리
- 데이터의 중요도에 따라 Compliance와 Enterprise 두 가지 모드 운영

데이터 관리의 편의성

- 스케일아웃 기반 스토리지로 멀티테넌시 제공
- 단일 가상 플랫폼에서 과장, 축소, 프로비저닝 등 가능
- 단일 플랫폼에서 애플리케이션 통합 및 분리 수용해 데이터 사일로 방지
- 중복 제거, 압축, 백업리스 환경, 이레이저 코딩 및 에러 복제 기능

신속성과 유연성

- 자동화된 데이터 티어링을 지원하며 프라이빗, 하이브리드 및 퍼블릭 클라우드 서비스 결합
- HDI 및 HCP Anywhere와의 결합을 통한 운영환경 개선