수탁사 개인정보 실태진단 서비스

Vendor Privacy Compliance Assessment Service

서면점검으로 확인하기 어려운 수탁사의 실제 개인정보 처리·보관·전송·삭제 현황을 현장에서 직접 검증합니다

HM COMPANY™

1. 수탁사 개인정보 실태진단의 필요성

개인정보보호에 대한 사회적 요구와 규제 수준이 높아지면서, 개인정보처리자의 관리 미흡은 단순 내부 문제가 아니라 법적 책임과 신뢰 훼손으로 이어지는 핵심 리스크가 되고 있습니다.
특히 **수탁사를 통한 개인정보 유출 사고가 지속적으로 발생**하면서, 위탁사의 수탁사 관리·감독 책임은 개인정보보호 체계의 핵심 관리 과제로 부상하고 있습니다.
개인정보 유출 또는 부적절한 처리는 정보주체의 권리 침해뿐 아니라 고객 신뢰 하락, 평판 훼손, 과징금·손해배상 등 복합적인 기업 리스크로 확대될 수 있습니다.
따라서 기업은 수탁사로부터 발생할 수 있는 개인정보 유·노출의 잠재 위험성을 예방하기 위해 **개인정보 관리 실태를 적극적으로 진단**할 필요가 있습니다.
수탁사 관리·감독은 계약 체결 시점의 확인만으로 충분하지 않으며, 개인정보가 실제로 **어디에 저장되고, 누가 접근하며, 어떻게 전송·보관·파기되는지**를 지속적으로 확인해야 합니다.

개인정보 처리에 대한 관리대책 법제화

양벌규정·감독의무 등
법적 책임 요구 강화

소비자의 개인정보 보안의식 저변 확대

개인정보 침해 민감도 증가,
사회적 감시 기반 확대

수탁사 통한 개인정보 유출 사고 증가

수탁사 유출 사고 증가,
위탁사 감독 책임 강화

관련 법령

개인정보보호법 제26조

업무위탁에 따른 개인정보 처리 제한

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, **처리현황 진단 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.**
⑦ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

개인정보보호법 제29조

안전조치의무

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 **내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치**를 하여야 한다.

2. 연도별 국내 개인정보 유출 현황

개인정보보호위원회 자료에 따르면,
2021년부터 2025년 10월까지 국내 개인정보 유출 규모는 약 1억 5,593만 건에 달하는 것으로 집계되었습니다.
이는 인구 5,114만 명 기준으로 환산할 경우, **국민 1인당 약 3건의 개인정보 유출**을 경험한 수준입니다.
특히 2025년 개인정보 유출 건수는 **7,516만 건**으로 2024년 593만 건 대비 약 **13배 증가**했으며, 대형 플랫폼·통신·서비스 기업 관련 사고가 집중적으로 발생했습니다.
수탁사 또는 협력사를 통한 개인정보 유출 사례도 지속적으로 확인되고 있어, 위탁사는 수탁사의 개인정보 처리 실태를 **실질적으로 관리·감독했는지 입증**할 수 있어야 합니다.

1.55억+ 건
2021 ~ 2025.10
5년간 국내 개인정보 유출 누적
개인정보보호위원회 / 머니투데이(2025)

13배
2024년 593만 건 → 2025년 7,516만 건
전년 대비 폭증
개인정보보호위원회(2025)

3.0건
5년 누적 유출 ÷ 인구 5,114만
국민 1인당 평균 유출 횟수
머니투데이(2025.12)

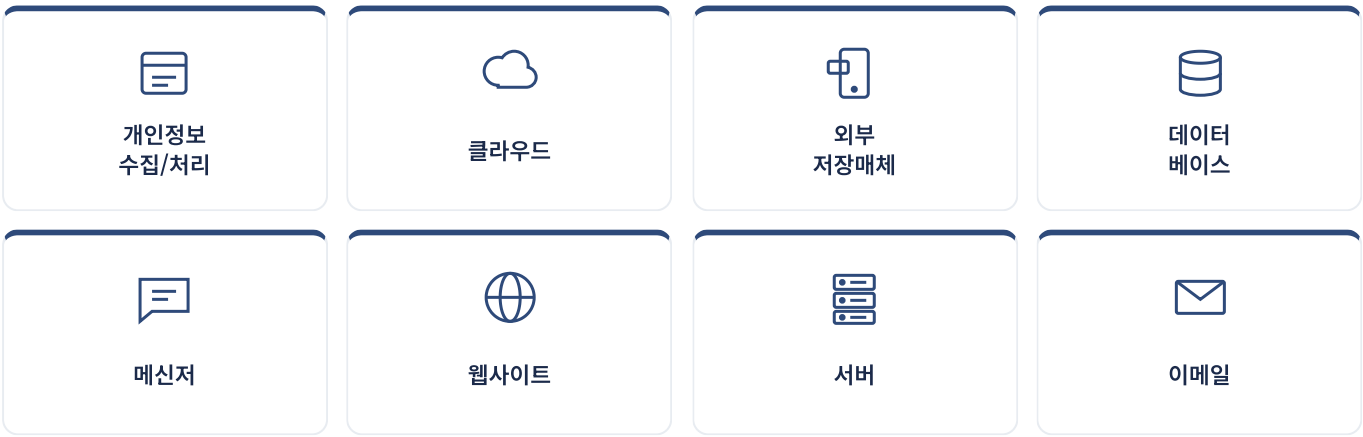
수탁사 부주의로 발생한 주요 유출 사례

'23.12	한양CC·서울CC	**골프장 회원 8만 7천여 명의 개인정보 외부 유출** 두 골프장 회원정보가 동일 서버·관리자 계정으로 통합 운영되어, 단일 계정 탈취만으로 전체 회원 정보 노출 (위·수탁자 모두 과징금 약 2억원)
'24.06	현대차·기아 협력사 S사	**1차 협력사가 보유한 위탁사 핵심 자료 다크웹 공개 협박** 시총 5,000억대 규모임에도 협력사의 보안 솔루션·백업·격리 체계가 충분치 않아, DB·재무·임직원 정보가 일괄 탈취됨
'24.10	현대차·기아 1차 협력사	**협력사를 통한 위탁사 신차 개발 정보 다크웹 노출** 신차 개발 일정·양산일·생산공장 등 영업비밀이 협력사 내부에 평문으로 저장된 채 보안 미흡한 환경에 노출됨
'25.04	KS한국고용정보	**콜센터 위탁 운영 중 임직원·지원자 약 4만 명 정보 유출** 외부에서 ID·비밀번호만으로 관리자 페이지 접속이 가능, 주민번호도 평문으로 보관되어 관리자 계정 탈취만으로 인사서류 전체가 빠져나감 (과징금 35.4억원)
'25.12	대한항공 (KC&D)	**기내식 협력사 서버 내 대한항공 임직원 약 3만 명 정보 유출** 위탁 종료·갱신 시 데이터 위치 통제와 파기 검증이 미흡하여 위탁사 정보가 협력사 서버에 잔존, 협력사 보안 미흡으로 해킹 피해 직결

참고자료: 뉴스1(2025.10), 보안뉴스(2024.06/10), 데일리시큐(2025.04), 아주경제(2025.12)

2. 개인정보 유·노출 잠재 위험성 요소 — 매체별 유형

HM COMPANY가 최근 1년간 다양한 업종의 50여 개 업체를 대상으로 개인정보 실태진단을 수행한 결과, **개인정보 수집·처리, 이메일, 웹사이트, 클라우드, 서버 등 다양한 업무 환경에서 개인정보 유·노출 위험 요소**가 확인되었습니다.
특히 상당수 위험 요소는 **담당자 본인도 인지하지 못한 임시파일, 로그, 캐시, 백업파일, 공유폴더 등**에 남아 있어 서면점검만으로는 식별하기 어렵습니다. 실제 **PC·서버·클라우드·업무시스템을 기준으로 한 현장 정밀진단**이 필요합니다.



유형별 주요 발견사항

유형	내용
개인정보 수집·처리	• 보관기간이 경과한 개인정보 파일 보관 • 개인정보 파일 암호화(DRM 설정) 및 자체 암호 미설정 • 사용자가 인지하지 못한 임시 저장 경로(AppData 하위 영역 등)에 개인정보가 포함된 파일 존재 • 업무용 프로그램의 로그 파일에 개인정보 문자열이 평문으로 저장
메신저 / 이메일	• 불필요하게 개인정보가 포함된 이메일이나 대화 내역을 보관 • 개인정보 미취급자에게 개인정보가 포함된 본문이나 첨부파일을 전송 • 보유기간이 경과한 이메일을 로컬 백업파일(PST 등)로 계속 보관
웹사이트 / 클라우드	• 상용 클라우드(네이버 MYBOX, 구글 Gmail, Microsoft OneDrive)에 개인정보 보관 • 웹브라우저 내 자동 로그인 설정 활성화 및 개인정보에 접근 가능한 계정정보 저장 • 웹브라우저 캐시 파일에 개인정보가 저장된 채 존재
서버	• 퇴사 임직원의 계정이 회수되지 않은 채 유지되어 외부에서 서버 접근 가능 • URL 파라미터 변조를 통해 로그인 절차 없이 내부 개인정보에 접근 가능 • 서버 운영 로그에 개인정보가 자동 기재된 채 지속적으로 존재
기타 저장매체 및 업무환경	• 완전삭제 미흡으로 인한 개인정보 파일 복구 • 비인가 외부저장매체를 통한 개인정보 파일 전송 이력 확인 • 접근제어 되지 않는 공유 폴더 또는 NAS 등에서 개인정보 파일 보관

2. 개인정보 유·노출 잠재 위험성 요소 — 보안 솔루션

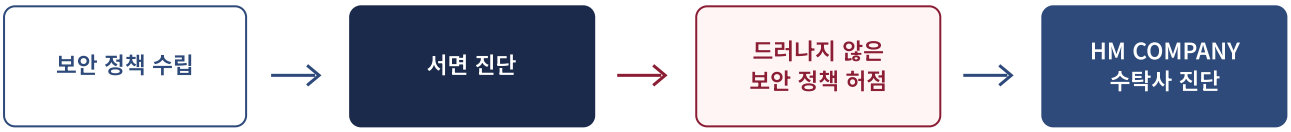
많은 기업이 개인정보 보호와 정보유출 방지를 위해 **DLP, 매체제어, 문서중앙화, 웹접속 차단 등 다양한 보안 솔루션**을 운영하고 있습니다.
그러나 보안 솔루션은 설정 범위, 예외 경로, 사용자 권한, 파일 변환 방식 등에 따라 **우회 가능성이 존재**하며, 인가된 사용자의 비정상 행위를 완전히 차단하기는 어렵습니다.
특히 운영 정책이 정교하게 관리되지 않는 경우, 다음과 같은 방식으로 **보안 솔루션의 탐지·통제 범위를 벗어날 수 있습니다.**
HM COMPANY의 수탁사 개인정보 실태진단은 보안 솔루션의 정책 설정과 실제 사용자 행위 흔적을 함께 분석하여, 단순 보관 미흡뿐 아니라 **우회 보관, 비인가 반출, 의도적 유출 정황**까지 확인합니다.

보안 솔루션 우회 유형

유형	내용
매체제어 우회	• USB 매체를 동시에 연결하거나 빠르게 탈부착을 반복하는 행위 • 매체제어 시스템의 탐지 범위를 벗어나는 외부저장매체를 사용하는 행위 • 인가된 외부저장매체에 데이터를 복사한 후 무단 반출하는 행위
파일탐지 우회	• 대상 파일의 확장자를 변경하거나 암호화하여 취급하는 행위 • 스크린샷 촬영, 파일 구조의 변경 등 다른 파일로 변환하여 사용하는 행위 • 보안 솔루션에서 예외 설정된 경로에 영업비밀 파일을 저장하여 탐지를 우회하는 행위
웹접속 탐지 우회	• VPN(가상사설망) 등과 같은 웹사이트 차단을 우회하는 수법을 사용하는 행위 • 블랙리스트에 포함되지 않은 URL을 사용하여 차단 대상인 웹사이트를 이용하는 행위
사회공학적 우회	• 기망 행위 등으로 접근 권한을 부정하게 취득하거나, 기한이 만료된 접근 권한을 계속 사용하는 행위

2. 개인정보 유·노출 잠재 위험성 요소 — 보안 정책

서면진단에서 양호한 결과를 받은 수탁사라도, 실제 현장에서는 **접근권한 관리, 보관기준 준수, 로그 관리, 파기 이행 등 보안 정책이 제대로 운영되지 않는 사례**가 빈번하게 확인됩니다.
개인정보는 **PC, NAS, 이메일, 메신저, 클라우드, 업무시스템, 로그파일 등 다양한 경로에 분산 저장**될 수 있으며, 담당자가 인지하지 못한 위치에 잔존할 가능성이 있습니다.
수탁사별 업무 범위와 IT 환경이 상이하기 때문에, 위탁사가 모든 수탁사의 **보안 정책 운영 상태를 직접 확인하는 데에는 현실적인 한계**가 있습니다.
HM COMPANY는 수탁사의 업무 프로세스, 접근권한, 저장매체, 보안 설정, 파기 이행 여부를 종합적으로 분석하여 **보안 정책의 운영상 허점을 식별하고 실행 가능한 개선안을 도출**합니다.

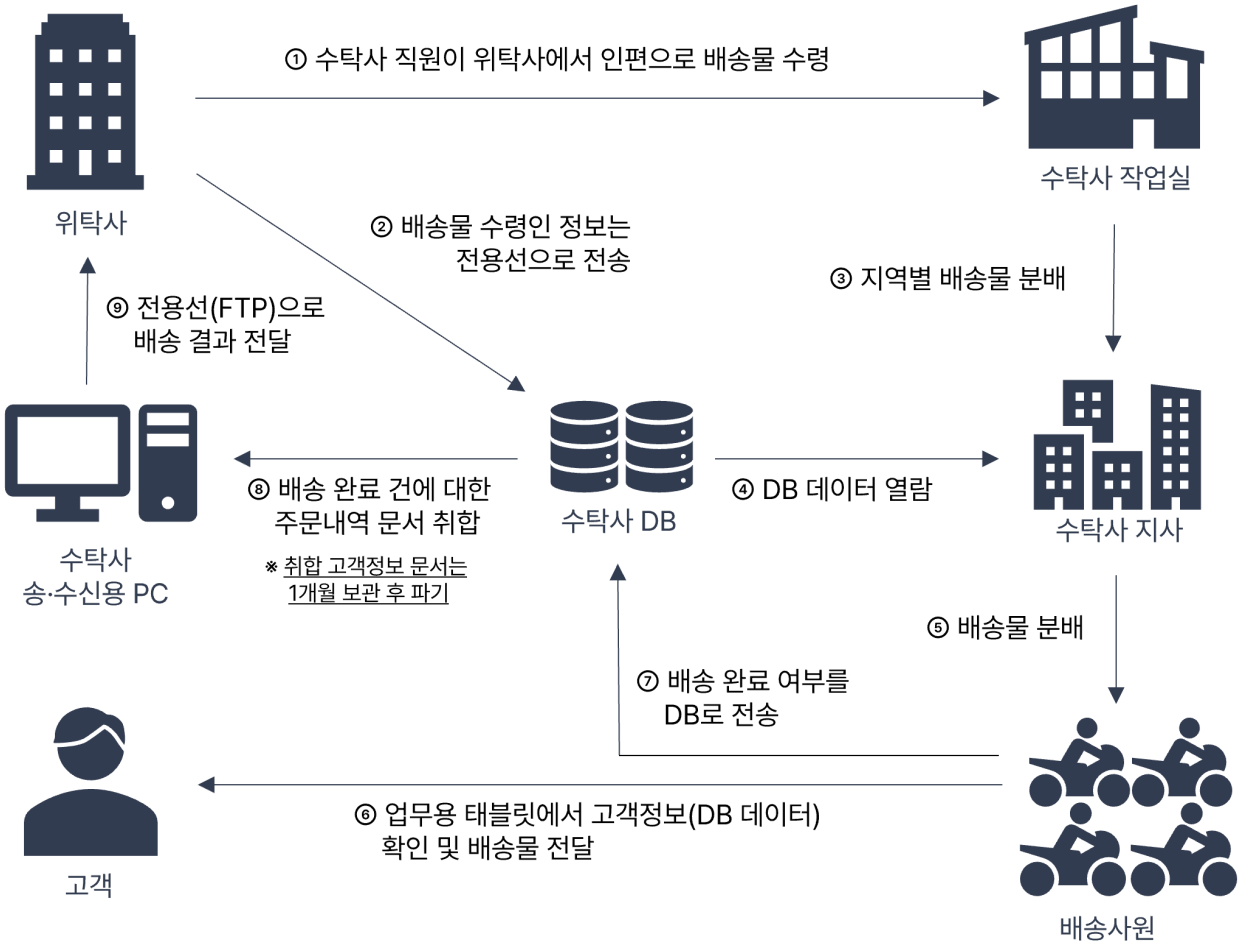


보안 정책 운영 미흡 유형

유형	내용
접근 제어 미흡	• NAS 내부 접근 권한이 분리되어 있지 않아 타 업무 실무자가 위탁 개인정보에 접근 가능한 환경 • 문서중앙화 솔루션 운영 시 팀별·취급자별 접근 권한이 분리되어 있지 않아, 개인정보 미취급자도 개인정보에 접근 가능한 환경
업무 프로세스 미흡	• 개인정보를 취급하지 않는 정산 담당자 등에게 개인정보가 포함된 자료를 전달하는 행위 • 사내 전자결재 시 개인정보 미취급 임원을 결재라인에 포함하여 개인정보 포함 품의서를 상신하는 행위 • 업무 매뉴얼·양식에 실제 고객 개인정보를 기재하여 사용하는 행위
보안 설정 및 관리 미흡	• 개인정보처리시스템에 접근 IP 설정이 되어 있지 않아 회사 외부에서도 접근 가능한 환경 • DRM 적용 범위 설정이 미흡하여 사진 등 일부 파일이 DRM 보호 대상에서 누락되는 환경 • 자체 구축한 사내 메신저의 대화 로그에 개인정보가 평문으로 저장되는 환경 • PC에 보안씰이 부착되어 있으나 시리얼번호가 기재되지 않아 위·변조 식별이 불가능한 환경

3. 수탁사 개인정보 진단 사례 — 배송 업무 ①

해당 사례는 **위탁사의 배송물 전달 업무를 대행하는 수탁사**로, 고객의 이름, 생년월일, 주소 등 개인정보를 제공받아 배송 업무를 처리한 사례입니다.

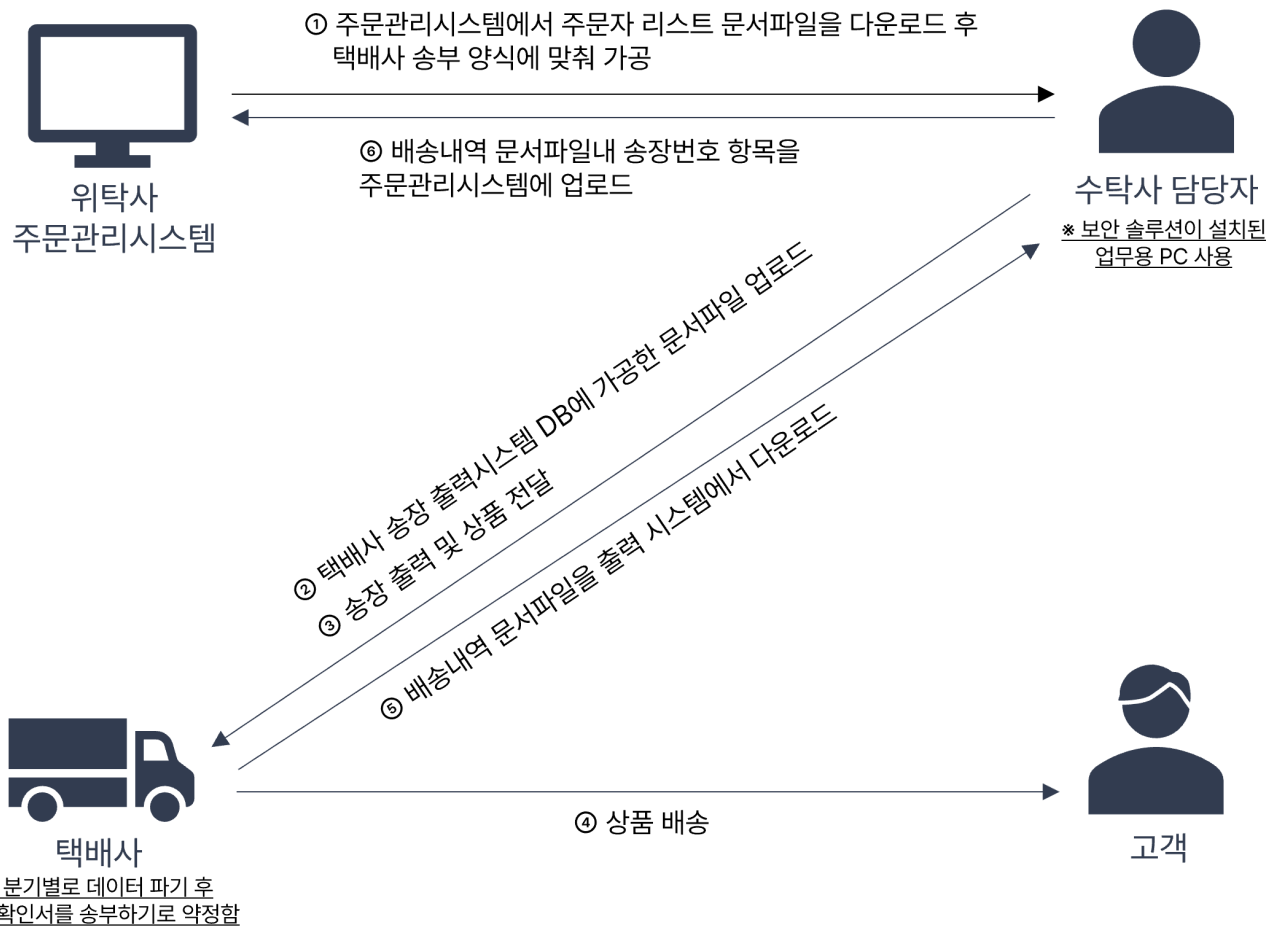


◆ 수탁사 개인정보 관리 실태 결과

항목	발견위치	발견사항
완전삭제	송·수신용 PC	• 삭제된 파일을 카빙 기법으로 복구한 결과, 고객 개인정보가 포함된 문서 및 이미지 파일이 잔존하고 있음을 확인
보관기준	송·수신용 PC	• 개인정보가 포함된 일부 업무 파일이 DRM 또는 자체 암호 설정 없이 평문 상태로 보관 • 약정된 보관기간이 경과한 개인정보 파일이 삭제되지 않고 보관
프로그램	송·수신용 PC	• 고객정보 송·수신에 사용되는 FTP 계정정보가 로그 파일에 평문으로 저장된 정황 확인
DB	수탁사 DB	• 마스킹 기준을 준수하지 않은 개인정보 항목이 DB 테이블 내 존재

3. 수탁사 개인정보 진단 사례 — 배송 업무 ②

해당 사례는 **상품 판매 및 배송 업무를 대행하는 수탁사**로, 고객의 이름, 주소, 휴대전화번호 등 배송 관련 개인정보를 위탁사로부터 제공받아 처리한 사례입니다.

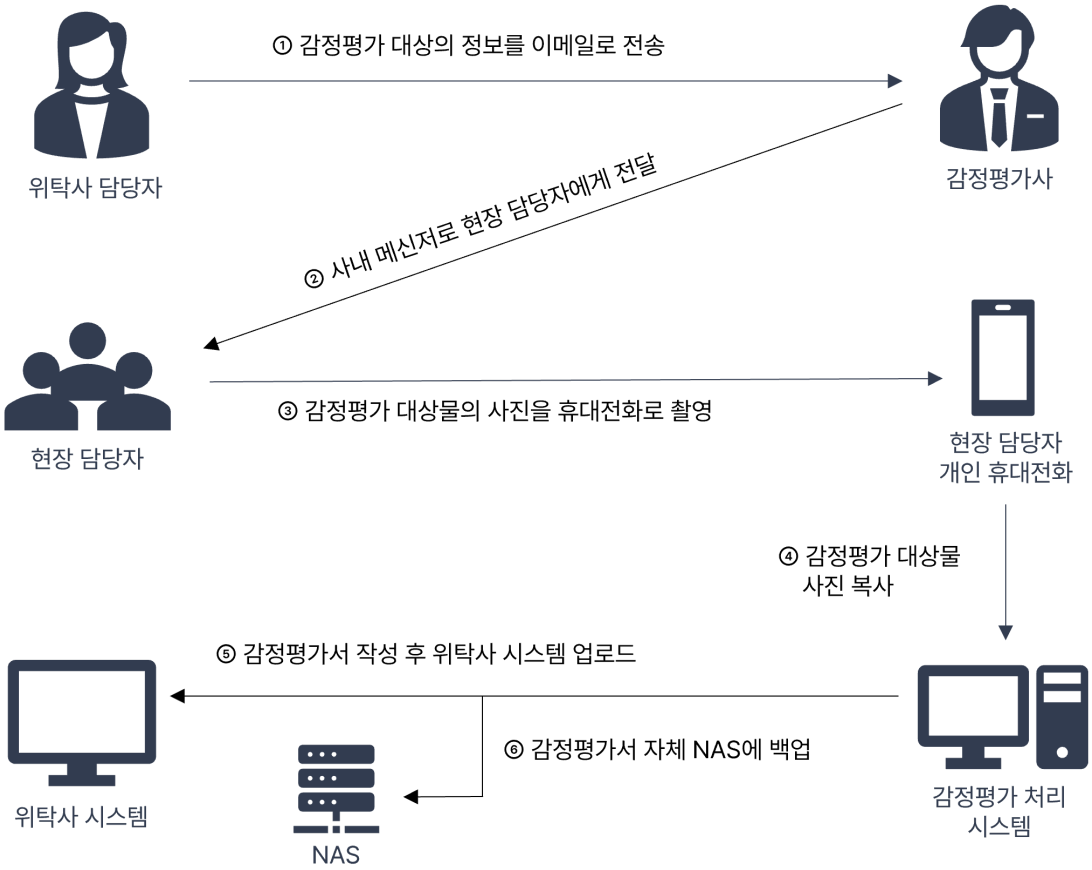


◆ 수탁사 개인정보 관리 실태 결과

항목	발견위치	발견사항
DB	택배사 DB	• 택배사로부터 분기별 파기확인서를 수령했음에도, 약정 보관기간을 초과한 고객정보가 DB 내 잔존
보안솔루션	담당자 PC	• 고객정보가 포함된 문서를 이미지 파일로 캡처한 뒤, 보안솔루션 탐지 예외 영역에 별도 보관
완전삭제	담당자 PC	• 삭제된 파일 복구 결과, 고객 개인정보가 포함된 문서 및 이미지 파일이 잔존
클라우드	담당자 PC	• 부서 공용 클라우드 저장공간에 고객 개인정보가 포함된 파일이 저장

3. 수탁사 개인정보 진단 사례 — 감정평가 업무

해당 사례는 **부동산 담보 평가 업무를 대행하는 수탁사**로, 고객의 이름, 생년월일, 휴대전화번호 등 감정평가에 필요한 개인정보를 위탁사로부터 제공받아 처리한 사례입니다.

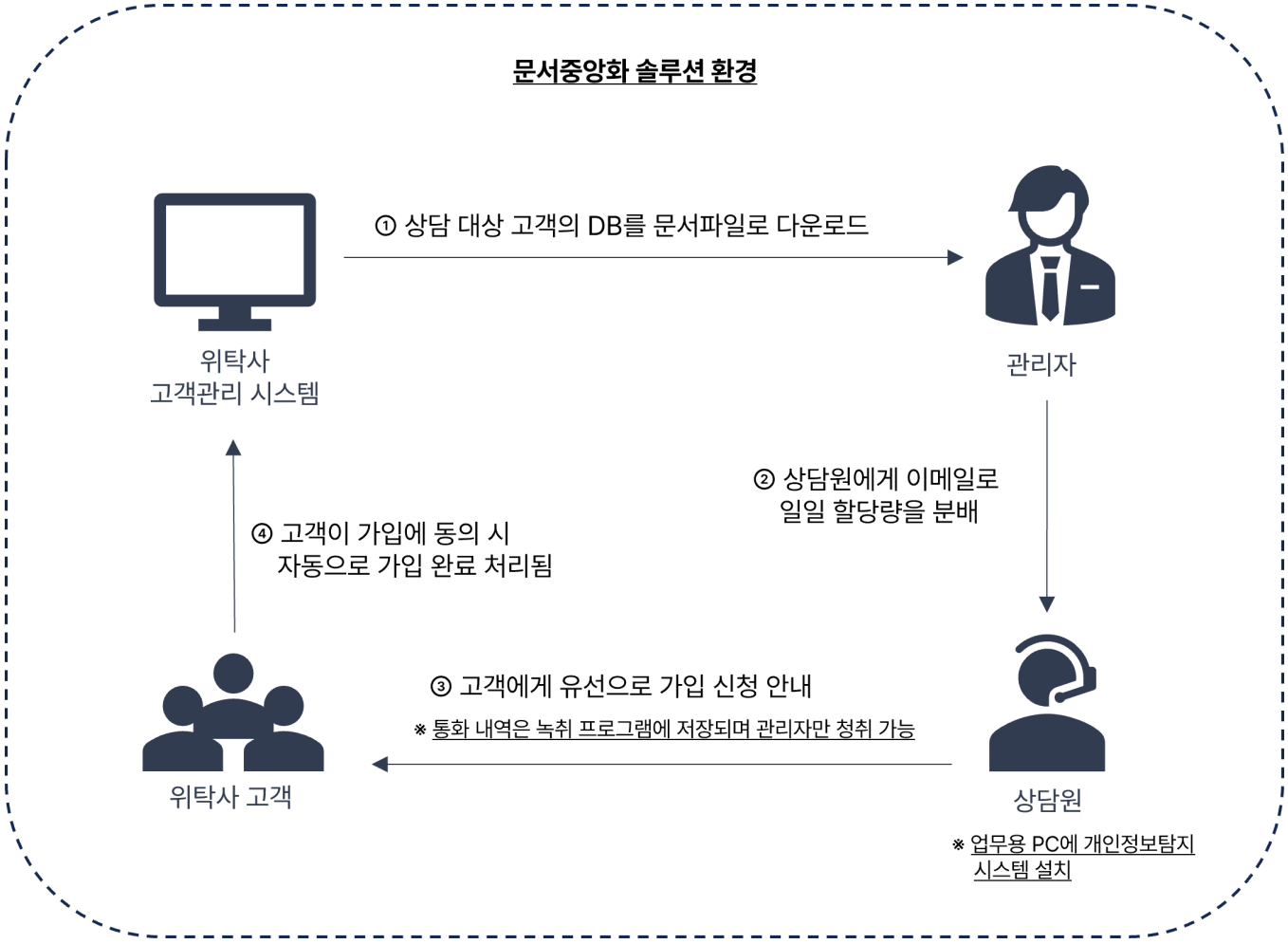


◆ 수탁사 개인정보 관리 실태 결과

항목	발견위치	발견사항
NAS	NAS	• 고객정보가 포함된 파일이 암호화 또는 별도 암호 설정 없이 저장 • 개인정보 취급 권한이 없는 사용자가 NAS 내 개인정보 파일에 접근 가능한 권한 구조 확인
메신저	감정평가사 PC 현장 담당자 PC	• 고객정보를 사내 메신저로 송수신한 대화 내역이 평문 로그 형태로 저장
보관기준	감정평가사 PC 현장 담당자 PC	• 개인정보가 포함된 업무 파일이 DRM 또는 암호 설정 없이 보관

3. 수탁사 개인정보 진단 사례 — 텔레마케팅 업무

해당 사례는 **금융서비스 상품 가입 상담 업무를 대행하는 수탁사**로, 고객의 이름, 생년월일, 계좌번호 등 금융 관련 개인정보를 제공받아 처리한 사례입니다.



◆ 수탁사 개인정보 관리 실태 결과

항목	발견위치	발견사항
보안솔루션	**관리자 PC**	• 개인정보가 포함된 다수의 문서가 개인정보탐지 시스템의 통제 범위를 벗어난 경로에 보관
보안기준	**관리자 PC**	• 문서중앙화 솔루션의 탐지 예외 영역에 개인정보 파일이 임시파일 형태로 저장
이메일	**관리자 PC**	• 고객정보가 포함된 이메일을 개인정보 미취급자에게 참조 발송
프로그램	**상담원 PC**	• 녹취 프로그램 사용 과정에서 생성되는 로그 파일에 고객정보가 평문으로 저장

4. 절차 및 기대효과

수탁사 개인정보 실태진단 서비스는 내부관리계획과 체크리스트 중심의 기존 서면진단을 넘어, **개인정보 취급자의 PC·모바일 기기·서버·NAS 등 실제 업무 매체를 분석**하여 개인정보의 보관·전송·잔존·파기 상태와 보안 규정 위반 가능성을 검증하는 **현장 기반 정밀진단 서비스**입니다.

기존 수탁사 진단

서면·자기진단 중심

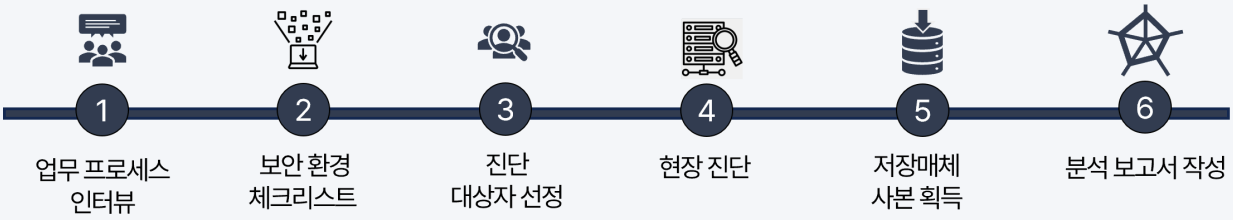
- 내부관리계획 문서 점검 위주
- 수탁사 자가진단·체크리스트에 의존
- 실제 매체에 남은 개인정보·우회 보관 발견 어려움
- 실제 개인정보 처리 현황 파악 한계

HM COMPANY 수탁사 진단

실제 매체 기반 정밀 진단

- PC·모바일·서버·NAS 등 매체 직접 분석
- 서면 점검 내용 대비 실제 개인정보 현황 비교 검증
- 보안솔루션·서버 등 시스템 취약점 식별
- 유출 위험 분석 및 개선 컨설팅 도출

수탁사 개인정보 실태진단 절차



1 업무 프로세스 인터뷰
업무 책임자·담당자 인터뷰로 개인정보 라이프사이클 기반 업무 흐름 확인

2 보안 환경 체크리스트
기술적·관리적 보호조치 기준에 준하여 자체 체크리스트 기반 준수 여부 확인

3 진단 대상자 선정
사내 조직도·업무 프로세스를 고려하여 고위험 직군을 대상자로 선정

4 현장 진단
대상자의 PC·모바일 기기·서버 등을 담당자 참관 아래 현장에서 진단 진행

5 저장매체 사본 획득
이미징 분석 대상자 저장매체 확보 후 사본 수집 (현장 분석 완료 후 별도 분석)

6 분석 보고서 작성
현장 진단 결과·이미징 분석 결과를 취합, 발견 사항에 대한 개선안 도출

진단을 통한 기대효과

위탁사

- ✓ 수탁사 보안 리스크에 대한 **선제적 대응**
- ✓ 개인정보 관리체계의 **실효성 강화**
- ✓ 실제 업무 절차 기준의 **개인정보 처리 현황 확인**
- ✓ 개인정보보호법상 **관리·감독 의무 이행 근거 확보**

수탁사

- ✓ 발견사항별 개선조치를 통한 **수탁사 보안환경 개선**
- ✓ 정기 진단을 통한 **수탁사 보안 인식 제고**
- ✓ 개인정보 관리 부실에 따른 **법적·평판 리스크 예방**

5. HM Company 주요 연혁 및 수행 실적

HM Company는 2011년 설립 이후 **디지털포렌식 전문성**을 기반으로 정보유출 조사, 개인정보·정보보호 리스크 진단, IT 감사, 내부감사 등 **기업 리스크 대응 서비스**를 수행해 왔습니다.

ADFS 본부	RAS 본부
디지털포렌식 서비스	컴플라이언스 리스크 진단
정보보호 리스크 진단	회계감사 외부전문가 조사
정보유출 조사	경영진단·내부감사
IT 감사	직장 내 괴롭힘 조사
KOLAS 공인 성적서 발행	PMA

주요 수행 실적

업체	분류	기간	내용
H 카드	금융	2011.10 ~ 현재	내부감사 Co-Sourcing
H 카드	금융	2012.07 ~ 현재	협력업체 개인정보 및 정보보안 포렌식 진단
W 반도체	제조	2025.07 ~ 2025.09	부정행위 조사
H 보험	금융	2024.12 ~ 2025.01	법인카드/골프회원권 부정 조사
H 바이오	의료	2023.10 ~ 2023.12	임원 부정행위 여부 조사
B 헬스케어	의료	2023.06 ~ 2023.09	자사 임직원 개인정보 관리실태 진단
L 반도체	제조	2023.05 ~ 2023.08	자체 첨단기술 등 영업 비밀 유출 진단
O 화학	제조	2022.11 ~ 2023.03	부정행위 조사
H 모터	제조	2022.06 ~ 2022.08	제품 설계도 등 영업 비밀 파일 유출 진단
L 에너지	제조	2022.02 ~ 2022.05	정보유출/부정 위험 조사
L 전자	제조	2022.02 ~ 2022.04	자사 서비스 가입 고객 개인정보 관리 컨설팅
H 제철	제조	2021.12 ~ 2022.06	회계장부 등 영업 비밀 유출 진단
M 유업	유통	2021.08 ~ 2021.11	자사 관리 고객정보 대상 실태진단
E 유통	유통	2021.05 ~ 2021.06	협력업체 대상 개인정보 실태진단

Why HM ADFS

15년+
디지털포렌식 기반
조사·진단 수행 경험

18,076+
누적 디지털 증거물 처리 경험
※ 국내 주요 대기업·금융·제조업체 포함

KOLAS
민간 최초 디지털포렌식분야
KOLAS 공인시험기관 인정

NDA
보안서약 체결,
데이터 안전 폐기 절차 운영

HM COMPANY™

Vendor Privacy Compliance Assessment Service

Contact Us

박 재 현 상무

jaehyun.park@hmcom.co.kr

이 정 훈 수석

jeonghoon.lee@hmcom.co.kr

대 표 전 화

02-6237-6233

수탁사 개인정보 실태진단 범위, 대상, 일정에 대한
상담과 맞춤 견적을 제공해 드립니다

hmcom.co.kr

hmadfs.com

서울특별시 서초구 효령로70길 36-9, 와이엘타워 2층, 3층