홈페이지 개인정보 노출방지 안내서

2018. 11

행정안전부
Ministry of the Interior and Safety

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

홈페이지 개인정보 노출방지 안내서

2018. 11

행정안전부
Ministry of the Interior and Safety

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

제·개정 이력

본 "홈페이지 개인정보 노출방지 안내서"는 2008년 2월 제정 이후 6차 개정판입니다.

구분	일자	비고
제정	2008.02	
1차 개정	2009.02	
2차 개정	2011.05	
3차 개정	2012.08	
4차 개정	2014.12	
5차 개정	2016.06	
6차 개정	2018.11	

홈페이지 개인정보 노출방지 안내서

- 본 안내서는 「개인정보 보호법」 등 관계 법령의 규정을 토대로,
  - 개인정보 담당자 및 홈페이지관리자를 대상으로 인터넷에 노출된 개인정보의 오남용을 예방하기 위하여 개인정보 노출 원인별 구체적인 사례 및 조치방법에 대한 올바른 이해를 돕기 위한 목적으로 발간되었습니다.
  - 다만, 다른 사람이 게시하거나 공개한 개인정보를 삭제할 때에는 임의 삭제 조치가 타인의 재산권 침해 등의 우려가 있는지 여부를 반드시 확인 후 조치해야 합니다.

- 본 안내서에서 제공하는 조치 방법 및 처리절차 예시 등은 각 기관의 고유한 특성 및 실제 환경에 맞게 적용하시면 됩니다.

본 안내서는 '개인정보보호 종합포털' 홈페이지 [https://www.privacy.go.kr 〉 자료마당 〉 지침자료]와 온라인 개인정보보호 포털 [https://i-privacy.kr 〉 자료실 〉 안내서 및 해설서]에 게시될 예정입니다.

CONTENTS

I 개요

1. 개인정보란? 8
   [여기서, 잠깐!] 일상생활에서 다양하게 활용되는 개인정보 10
2. 개인정보 노출의 이해 11
   가. 개인정보 노출의 위험성 11
   나. 언론보도로 보는 개인정보 노출 13
   다. 숫자로 보는 개인정보 노출 19

II 개인정보 노출원인 및 조치방안

1. 홈페이지관리자 부주의에 의한 노출 23
   가. 관리자페이지 접근제어 미흡 23
   [여기서, 잠깐!] 관리자페이지 안전하게 보호하기 24
   나. 개인정보가 포함된 게시물 등록 27
   다. 개인정보가 포함된 게시글 및 댓글 게시 28
   라. 개인정보가 포함된 첨부파일 게시 30
   [여기서, 잠깐!] 개인정보 노출의 원인이 되는 엑셀 기능 알아두기 35
2. 이용자 부주의에 의한 개인정보 노출 45
   가. 개인정보가 포함된 게시글 및 댓글 작성 45
   나. 개인정보가 포함된 첨부파일 게시 48
3. 홈페이지 설계 및 개발 오류에 의한 노출 50
   가. 홈페이지 접속경로(URL) 관련 오류 50
   [여기서, 잠깐!] GET 방식과 POST 방식 알아보기 54
   나. 홈페이지 소스코드 보안설정 미흡 55
   다. 임시 저장 페이지 미삭제 57
   라. 디렉터리 리스팅 보안설정 미흡 59

4. 검색엔진을 통한 개인정보 2차 노출 61
가. 검색엔진의 이해 61
나. 검색엔진별 개인정보 노출 조치방안 62

III 개인정보 노출, 예방할 수 있습니다!

• 홈페이지 운영자 개인정보 노출 예방수칙 80
• 홈페이지 개발자 개인정보 노출 예방수칙 85

FAQ 무엇이든 물어보세요 90

부록

[부록 1] 주요 용어 이해하기 98
[부록 2] 개인정보 노출 점검, 스스로 해보기 101
[부록 3] 개인정보 유출 시 필수 조치사항 104
[부록 4] 주요 개인정보 8종 정규표현식 115
[부록 5] 참고자료 116

홈페이지 개인정보 노출방지 안내서

I

개요

1. 개인정보란?
2. 개인정보 노출의 이해

I 개요

1. 개인정보란?

'개인정보'란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말하며, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보가 포함됩니다(「개인정보 보호법」 제2조제1호).

예를 들어, 주민등록번호는 우리 국민 개개인마다 고유하게 부여되는 것으로(개인정보 보호법 상 '고유식별정보'로 불림) 개인을 손쉽게 식별하는데 활용할 수 있으므로, 그 자체로도 개인정보라 할 수 있습니다. 그러나 생년월일, 주소, 전화번호 등은 해당 정보만 독자적으로 노출되었을 때에는 개인을 알아볼 수 없지만, 다른 정보와 결합하면 특정 개인을 식별할 수 있게 되므로 개인정보로 볼 수 있습니다.

이처럼 개인정보는 성명, 주민등록번호, 생년월일, 주소, 전화번호 등의 기본 인적 사항에서부터 지문·홍채 등 신체정보(바이오정보), 의료·건강정보, 학력·성적 등 교육정보, 소득·신용등급 등 금융·신용정보, 사회·경제적 지위와 정치적 성향과 같은 내면의 비밀에 이르기까지 그 종류가 매우 다양하고 폭넓습니다. 또한, 기관·기업에서 운영하는 홈페이지 등에 회원으로 가입하거나 등록할 때 이용자로부터 직접 수집하는 정보뿐만 아니라, 이용자가 홈페이지나 서비스를 이용하는 과정에서 자동 생성되는 접속기록(로그), 통화내역, 상품 구매내역, GPS 위치정보 등도 개인정보가 될 수 있습니다.

일반적 정보
• 주민등록번호
• 이름, 주소, 전화번호
정신적 정보
• 기호, 성향
• 신념, 사상
통신·위치 정보
• 통화, IP주소
• GPS 등
신체적 정보
• 신체정보
• 의료, 건강 정보
사회적 정보
• 교육 정보
• 근로 정보
• 자격 정보
재산적 정보
• 개인 신용정보
• 부동산, 주식

[그림 1] 개인정보 종류

여기서, 잠깐!

일상생활에서 다양하게 활용되는 개인정보

[그림 2] 일상생활에서 개인정보의 활용

2. 개인정보 노출의 이해

가. 개인정보 노출의 위험성

개인정보 노출이란 인터넷 상에서 누구든지 해킹 등의 특별한 방법을 사용하지 않고도 홈페이지 등을 통해 타인의 개인정보를 손쉽게 확인·조회하거나 취득할 수 있도록 개인정보가 공개 또는 방치되어 있는 상태를 말합니다.

인터넷 상에 노출되는 개인정보는 이름, 생년월일, 주소, 전화번호, 이메일 주소 등의 기본정보 뿐만 아니라, 주민등록번호 및 여권번호, 운전면허번호, 외국인등록번호와 같은 고유식별정보, 더 나아가 통장 계좌번호, 신용카드 번호, 건강보험번호 등에 이르기까지 매우 다양하게 나타나고 있습니다.

[그림 3] 개인정보 노출 예시

개인정보 노출이 발생하게 되면, 개인의 경우 사생활침해, 명의도용, 불법스팸, 보이스피싱 등에 의한 경제적·정신적 피해를 야기할 뿐만 아니라 노출된 개인정보가 각종 범죄에 악용될 우려가 있으며, 기관·기업의 경우에도 고객 신뢰 상실, 이미지 실추, 소비자단체 등의 불매운동, 더 나아가 소송이나 손해배상 등 유·무형의 피해를 입을 수 있습니다.

최근 정부에서는 인터넷 상 우리 국민의 개인정보를 보호하고 노출 등으로 인한 피해 확산 방지를 위해 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 개정, 정보통신서비스 제공자 등의 개인정보 노출 방지 및 노출된 개인정보의 삭제·차단 조치 의무를 규정한 바 있습니다(2016. 3월 신설). 따라서, 홈페이지를 운영하는 기관·기업에서는 내부 직원 교육을 통한 인식 제고와 함께 홈페이지 상 개인정보 작성 시 주의 안내, 지속적인 노출 모니터링 실시 등 각별한 주의가 필요합니다.

참고

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 상의 개인정보 노출 관련 조항

제32조의3(노출된 개인정보 삭제·차단) ① 정보통신서비스 제공자등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다.

② 정보통신서비스 제공자등은 방송통신위원회 또는 한국인터넷진흥원의 요청이 있는 경우 제1항의 노출된 개인정보에 대한 삭제·차단 등 필요한 조치를 취하여야 한다.

나. 언론보도로 보는 개인정보 노출

2018년 7월 2일

A여행사, 여권번호, 신용카드 등 개인정보 줄줄이 노출

특정 여행사 사이트 여권번호,카드번호,연락처,이름 등 개인정보 무방비 노출

국내 여행사 사이트에서 여권번호·카드번호·연락처 등 중요한 개인정보가 노출되는 사건이 발생했다. 특히, 개인정보는 암호화되지 않고 여행사 홈페이지를 비롯해 구글 검색 등을 통해 그대로 노출된 것으로 드러났다. 더욱이 해당 여행사의 웹서버에 지난 2015년부터 저장돼 있었다는 의혹까지 제기되면서 개인정보 관리 부실이 또 다시 도마 위에 올랐다.

(생략)

문제가 된 해당 여행사의 예약확인 화면을 본지가 확인한 결과, 카드 결제금액, 승인번호 8자리, 카드번호, 카드 유효기간, 할부기간, 생년월일 6자리가 그대로 노출돼 있다. 여기에다 예약확인 여권정보, 현금영수증 정보 등까지 클릭할 수 있다.

(생략)

특히, 여권번호와 카드번호, 유효기간, 비밀번호 등은 개인 신용정보와 직접적으로 연관돼 있어 금전적 피해는 물론 2,3차 피해까지 발생할 수 있어 매우 위험하다. 더욱이 비행 출발시각, 도착시각, 비행편명 등의 정보까지 노출돼 있어 각종 위험에 노출될 수 있다. 무엇보다 이러한 중요 개인정보가 암호화 조치 없이 관리되고 있다는 것은 개인정보보호법 안전성 확보조치 위반에 해당된다.

이와 관련 한 기업의 CISO는 "이번 사건은 이용자의 주요 정보가 모두 노출됐다는 점에서 프라이버시 침해의 심각성이 매우 크다고 볼 수 있다"며 "제3자에게 공개되는 경우, 신원 도용(Identity theft)에 활용할 수 있는 정보가 버젓이 노출되어 있다. 또한, 이용자의 여행 경로가 노출되어 제3자에 의한 협박 및 갈취 등 2차 피해가 우려되는 문제점이 있다. 게다가 DB뿐 아니라 웹서버에 파일의 형태(.html 포함)로 개인정보가 방치되고 있다는 점은 개인정보 관리가 얼마나 허술했는지 알 수 있다는 점에서 근본적인 개선이 필요하다"고 지적했다. (생략)

출처 : 보안뉴스 http://www.boannews.com/media/view.asp?idx=70904&kind=1
김경애 기자 boan3@boannews.com

2016년 7월 18일

A사 홈페이지에 고객정보 노출

A사 홈페이지에 고객정보가 노출돼 일반 승객들의 개인정보 유출 우려가 나온다.

A사는 18일 홈페이지 고객센터 내 '자주 묻는 질문들'(FAQ) 부분에 이용자가 올린 게시글의 첨부파일 접속주소(URL)가 노출되는 오류가 발생됐다고 밝혔다. 이 파일에는 여권과 주민등록증 등 개인 신상정보도 일부 포함돼 주소를 누르면 이를 볼 수 있다.

회사 측은 지난해 5월 이후 고객센터 FAQ에 등재된 4만7023건의 게시글 중 일부 이용자의 첨부파일이 노출됐을 가능성이 있다고 판단, 외부 유출 여부를 확인 중이다. 지금까지 외부에서 조회된 사례는 지난 15일 1건으로 파악됐다는 것이 A사 측의 설명이다. 회사 측은 유출 사실을 진지한 이날 오전 고객센터 FAQ 서버 운영을 중단하고 긴급 점검을 벌이고, 한국인터넷진흥원(KISA)에 해당 사안을 신고했다.

A사 관계자는 "홈페이지 전체 회원의 정보가 노출된 것은 아니다"라며 "구체적인 피해 여부를 확인하고 있으며 해당 고객들에게 사과드릴 것"이라고 말했다.

출처 : 경향신문 http://biz.khan.co.kr/khan_art_view.html?artid=201607181854001&code=920100
김보미 기자 bomi83@kyunghyang.com

2016년 5월 7일

MTB 대회 참가했다가... 블로그·포털에 노출되는 개인정보

블로그 및 카페 운영진, 회원 개인정보 노출 각별히 주의해야

전국 산악자전거대회 - 참가자 명단(배번,칩,사이즈)

접수번호	배번	이 름	생년월일	휴대전화	참 가 종 목	팀 명	상의사이즈
793	101	신[illegible]	820[illegible]	010-[illegible] 04[illegible]	xc 46km 중급남자 베테랑	바이크브라더스	XL
405	102	염[illegible]	760[illegible]	010-[illegible] 93[illegible]	xc 46km 중급남자 베테랑	팀 익스피드	S
154	103	이[illegible]	820[illegible]	010-[illegible] 8[illegible]	xc 46km 중급남자 베테랑	팀 불꽃	S
88	201	김[illegible]	7005[illegible]	011-[illegible]	xc 46km 중급남자 마스터	일반	L
598	202	김[illegible]	7107[illegible]	010-[illegible] 55[illegible]	xc 46km 중급남자 마스터	청주 블루이글스	S
731	203	류[illegible]	7112[illegible]	010-[illegible] 8[illegible]	xc 46km 중급남자 마스터	수원알파	L
687	204	박[illegible]	681[illegible]	010-[illegible] 0336	xc 46km 중급남자 마스터	팀 매드라이더스	S

구글 검색을 통해 개인정보를 비롯한 중요 정보가 노출되는 사례가 계속 이어지는 가운데 이번에는 생년월일과 휴대폰번호 등 개인정보가 대거 포함된 특정 MTB 대회 참가자 명단이 블로그에 게시되어 있고, 이것이 포털 검색을 통해 무방비로 노출돼 문제가 커지고 있다.

이는 특정 휴대전화번호인 '010-7**9-69**'를 네이버에 검색할 경우 한 개인이 개설한 블로그에 수십명의 이름, 생년월일, 핸드폰번호 등 민감한 개인정보가 포함된 문서가 무방비로 노출된다는 제보를 본지가 확인하는 과정에서 드러났다.
(생략)
해당 블로그는 다음에 개설한 MTB 관련 개인 블로그였고 노출된 개인정보는 지난해 MTB 관련 대회 참가자 명단으로 추정된다. 또한, 구글 검색에서 '2015. 제3회 **시 **산 전국 산악***대회 ***'로 검색해도 동일한 문서가 노출된다.

이는 개인정보에 대한 무관심과 보안의식 부족이 주요 원인으로, 인터넷 동호회나 개인 블로그, 카페 등을 통해서 개인정보가 노출될 경우 2차 피해로 이어질 수 있다. 노출된 정보를 악용해 보이스피싱이나 금융사기 등 사이버범죄의 주요 타깃이 될 수 있기 때문이다. (생략)

출처 : 보안뉴스 https://www.boannews.com/media/view.asp?idx=50528&page=1&kind=3
김태형 기자 boan@boannews.com

2018년 6월 1일

OO시, 탈북 직원 10여명 신상정보 노출…
“해당 직원 실수”

탈북민 출신의 OO시 산하기관 직원에 대한 신상 정보가 OO시 홈페이지에 넉 달 가까이 게재된 것으로 31일 드러났다. 탈북민의 개인정보 보안은 북한의 남은 가족의 신변에 직결되는 문제라 특히나 민감한 부분이다.

이날 OO시는 지난 1월28일 OO교통공사가 시로 보낸 ‘북한이탈주민 채용현황 제출’ 문서가 지난 28일까지 시 홈페이지 ‘정보소통광장’에 공개됐다고 밝혔다. 정보소통광장은 OO시에서 생산 · 결재한 모든 문서를 시민에게 공개하는 사이트이다. 개인정보 등 민감한 정보를 담은 문서는 부분공개 또는 비공개 처리된다.

해당 문서에는 OO교통공사 측이 채용한 탈북민 출신 직원 10여 명의 이름과 성별, 생년월일, 채용일자, 정착기간 등 11가지 개인신상 정보가 포함됐고, 검색하면 누구든 볼 수 있는 ‘공개’ 상태였던 것으로 확인됐다.

문서를 전부 공개로 설정해 올린 OO교통공사는 해당 문서를 OO시에 제출하는 과정에서 ‘비공개’로 설정해야 했으나 ‘담당자 실수’로 공개 처리됐다고 해명했다. 또 현재까지 이 문서가 30건 정도 조회된 것으로 나타나 비공개 처리했는데, 다행이 개인정보 노출에 따른 피해는 없었다고 덧붙였다.

OO시 관계자는 “산하기관이 결재한 문서의 공개 여부는 시스템상 해당 기관에서 설정하도록 돼 있다”며 “시 홈페이지 하루 이용자 수가 만 명에 달하는 만큼 개인정보 노출 방지를 위해 필터링 프로그램을 강화하겠다”고 밝혔다.

출처 : 중앙일보 https://news.joins.com/article/22676141
한영혜 기자 han.younghye@joongang.co.kr

2016년 2월 22일

구글에 무방비 노출되고 있는 개인정보 4천여건 확인

주민등록번호, 계좌번호, 휴대폰 번호, 주소, 집전화번호, 이메일 주소 등 노출

구글에 여전히 한국인 주민등록번호를 포함한 각종 개인정보가 무방비로 노출되고 있어 심각한 상황이 지속되고 있다. 노출되는 파일들은 누구나 다운로드 가능하며 이를 악용한 2차적인 피해로 이어질 수 있다. 개정된 개인정보보호법이 지난 2014년 8월 시행된 이후 데일리시큐는 구글 검색만으로 노출되고 있는 개인정보 문제를 지속적으로 기사화했지만 고쳐지지 않고 있다.

이번에 노출이 확인된 개인정보 파일에는 이름, 주민등록번호, 계좌번호, 휴대폰 번호, 주소, 집전화번호, 이메일주소 등 다양한 정보들이 포함돼 있다. 개인정보보호법에 따르면 해당 개인정보처리자는 유출 사실을 지체없이 정보주체에 알려야 하고 과징금이 부과되어야 하며 정보주체는 법정손해배상을 청구할 수 있는 사안이다.
(생략)
"엑셀파일 이외 워드파일이나 PDF 파일 등 다양한 형태로 개인정보가 노출되고 있고 누구나 다운로드 가능한 상황이라 2차 피해가 우려된다"며 "시스템에 보유하고 있는 개인정보가 유출되지 않도록 하는 것도 중요하지만 이처럼 이미 노출되고 있는 개인정보에 대해서도 또 다른 피해로 이어지지 않도록 각별한 신경을 썼으면 하는 바람이다"라고 말했다. (생략)

출처 : 데일리시큐http://www.dailysecu.com/?mod=news&act=articleView&idxno=13000&sc_code=&page=&total=
길민권 기자 mkgil@dailysecu.com

2017년 6월 15일

온라인 쇼핑몰 W사 누리집서 회원 개인정보 노출

14일 오후 환급 신청자 계좌번호 등 5시간 가량
W사, "누리집 업데이트 과정서 실수로 100여건 노출,
이용자들 자료 형태를 볼 때 3만 5천여건 노출" 추산

국내 3대 온라인쇼핑몰 업체 중 하나인 W사 회원 수만명의 개인정보가 누리집에 5시간 가량 노출됐다.

15일 W사 이용자들의 말을 들어보면, W사 회원들의 환급 금액과 은행 계좌번호 등이 14일 오후 1시쯤부터 5시간 가량 누리집의 포인트 내역을 조회하는 난에 노출됐다. 환급 상태를 클릭하면 회원 이름도 보여졌다. W사는 100여건이라고 설명하지만, 이용자들은 3만5천건 이상 노출된 것으로 추산한다.

W사는 "누리집을 업데이트하는 과정에서 실수가 있었다. 회원들의 항의를 받은 뒤 즉각 오류를 수정했다"고 밝혔다. 하지만 15일 밤까지도 누리집에 공지나 사과문을 올리지는 않았다. 이 업체는 2014년에도 사용자이름(아이디) 도용으로 회원 300여명의 포인트 1100만원어치를 도난당한 바 있다.

출처 : 한겨레 http://www.hani.co.kr/arti/economy/it/799062.html#csidx83037b691bf753a8fb5dda3ca965378
김재섭 기자 jskim@hani.co.kr

다. 숫자로 보는 개인정보 노출

공공부문 홈페이지를 통한 개인정보 노출 추이를 살펴보면, 2012년에 개인정보 노출 홈페이지 수는 총 1,164개로 개인정보 노출이 가장 많이 발생하였으며, 이듬해인 2013년 개인정보 노출 홈페이지 수는 크게 감소하여 727개로 나타났습니다.

이후 개인정보 보호법이 본격 시행되고 주민등록번호 등 주요 개인정보 처리에 대한 규제가 강화되면서 홈페이지를 통한 개인정보 노출은 지속적인 감소세를 보이고 있으며, 2017년에는 개인정보 노출 홈페이지 수는 398개로 최저치를 경신한 바 있습니다.

[그림 4] 공공부문 개인정보 노출 홈페이지 건수

[그림5]는 최근 3년간('15년~'17년) 발생한 공공부문 홈페이지 개인정보 노출 원인을 분석한 결과입니다. 그 결과 개인정보 노출의 주된 원인으로는 '홈페이지관리자 부주의'가 총 49%(860건)로 약 과반수를 차지했으며, 다음으로 '홈페이지 이용자 부주의'가 39%(697건) 차지했던 것으로 분석되었습니다.

홈페이지관리자 부주의로 발생한 개인정보 노출의 경우에는 '개인정보가 포함된 첨부파일 등록'이 82%(704건)로 거의 대부분을 차지했으며, '개인정보가 포함된 게시글/댓글 작성'을 통한 노출도 15%(126건) 차지했습니다.

한편, 홈페이지 설계 및 개발 오류로 발생한 개인정보 노출은 총 12%(210건)으로

상대적으로 적은 편이었으나, 대규모 개인정보 노출의 주된 원인이 되고 있으므로 홈페이지 설계·개발 단계부터 각별한 주의가 필요합니다.

[그림 5] 공공부문 홈페이지 개인정보 노출 원인

II

개인정보 노출원인 및 조치방안

1. 홈페이지관리자 부주의에 의한 노출
2. 이용자 부주의에 의한 개인정보 노출
3. 홈페이지 설계 및 개발 오류에 의한 노출
4. 검색엔진을 통한 개인정보 2차 노출

II 개인정보 노출원인 및 조치방안

[그림 6] 개인정보 노출원인 및 조치방안

1. 홈페이지관리자 부주의에 의한 노출

가. 관리자페이지 접근제어 미흡

홈페이지에 가입한 정보주체의 개인정보를 조회·변경·다운로드할 수 있는 관리자페이지는 인가된 홈페이지관리자만 접속할 수 있도록 구축·운영되어야 합니다. 가입된 모든 정보주체의 개인정보를 처리할 수 있는 관리자페이지가 인터넷에 노출될 경우, 일반적인 개인정보 노출 사례와 달리 대량의 개인정보가 노출될 수 있으므로 각별한 주의가 필요합니다.

노출사례

A공공기관은 내부망에서만 접근 가능하도록 관리자페이지를 설계하였습니다. 하지만 외근이 많았던 홈페이지관리자는 외부 출장 시에도 관리자페이지에 접근하기 위해 외부망에서도 접근 가능하도록 설정을 변경하였습니다. 이후 홈페이지관리자는 내근 시에는 외부망 접근 설정, 외근 시에는 외부망 접근을 해제하는 식으로 업무를 진행했습니다. 홈페이지관리자가 외근 중 불의의 사고를 당하였고 이로 인해 접근제어 설정이 원상복구되지 않아, 관리자페이지가 외부망에서 접근 가능하도록 방치되었습니다. 때마침 개발자의 실수로 관리자페이지의 비밀번호 설정이 해제되었고 해당 홈페이지 내 개인정보가 관리자페이지를 통해 대량 노출되었습니다.

[그림 7] 관리자페이지 접근제어 미흡으로 노출된 사례

조치방법

상기 사례는 ① 관리자페이지에 대한 외부 접근제어 ② 관리자페이지 로그인 비밀번호 설정이 제대로 되지 않아 개인정보가 노출된 건입니다. 만일 두 가지 사항 중 한 가지 사항만 적용되었더라도 개인정보 노출이 발생하지 않았을 것입니다.

특히, 개인정보 보호법 제29조에 의하면 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용해야 합니다. 관리자페이지에 접속하는 경우도 개인정보처리시스템에 접속하는 것으로 인정되는 바, 상기 의무사항이 관리자페이지 접속 시에도 적용됩니다.

따라서 개인정보처리자는 ▲관리자페이지를 정보통신망을 통해 외부에서 접속할 경우 안전한 접속수단 혹은 안전한 인증수단 마련 ▲관리자페이지 접속 주소가 ~/admin, ~/administrator 등 예측하기 쉬운 주소가 아닌지 체크 ▲디폴트 비밀번호 및 쉬운 비밀번호 사용 지양 등의 사항을 준수해야 합니다.

NOTE!

홈페이지별로 관리자페이지에 적용되어 있는 접근제어 조치가 상이할 수 있습니다. 상기 내용을 참조하여 보다 안전하게 관리자페이지를 관리하시기 바랍니다. 자세한 사항은 '[여기서, 잠깐!] 관리자페이지 안전하게 보호하기'를 참고하시기 바랍니다.

여기서, 잠깐!

관리자페이지 안전하게 보호하기

관리자페이지에서 개인정보 노출을 방지하기 위해, 개인정보처리자는 홈페이지관리자가 외부에서 관리자페이지에 접속할 경우 안전한 접속수단 혹은 안전한 인증수단을 마련해야 합니다. 전용선 및 가상사설망(VPN)을 통해 관리자페이지에 접속할 수 있도록 접근제어하거나, 혹은 휴대폰인증 및 공인인증서, OTP 등 추가 인증(2-Factor 인증)을 통해 접속할 수 있도록 해야 합니다.

[그림 8] OTP

[그림 9] 휴대폰인증

[그림 10] 공인인증서

만일 예산 부족 등으로 상기 안전한 접속수단 및 추가인증수단을 마련할 수 없는 경우, 관리자페이지에 대한 접속 권한을 IP주소 등으로 제한하여 접근자체를 원천적으로 차단할 수 있습니다. 다만, 이 경우 해당 단말기(접속권한이 있는 IP를 부여받은 PC)가 다수의 사용자에 의해 이용되거나, 네트워크를 통해 원격 접속되지 않도록 관리해야 합니다.

※ 자세한 내용은 'ⅲ. 개인정보 노출, 예방할 수 있습니다!'

[그림 11] 관리자페이지 접근제한(특정 IP만 접속 허용)

또한 개인정보처리자는 홈페이지에 관리자페이지의 주소를 링크로 만들어서는 안 되며, 관리자페이지의 주소를 쉽게 추측 가능한 주소로 사용하지 말아야 합니다.

[그림 12] 관리자페이지의 링크

[그림 13] 추측 가능한 관리자페이지

마지막으로 개인정보처리자는 홈페이지관리자가 디폴트 비밀번호 및 쉬운 비밀번호를 사용하지 못하도록 관리해야 하며, 주기적으로 이를 점검해야 합니다.

[그림 14] 최초 로그인 시 비밀번호 변경

[그림 15] 안전한 비밀번호가 아닐 경우

나. 개인정보가 포함된 게시물 등록

홈페이지를 운영하는 개인정보처리자는 정보주체의 개인정보가 포함된 페이지가 생성되어 인터넷에 노출되지 않도록 관리·감독해야 합니다.

노출사례

온·오프라인 강의 사업자인 A학원은 홍보를 위해 강사의 경력정보를 홈페이지에 공개하고 있는데, 신입강사 채용으로 인한 홈페이지 개편 시 신규 강사의 운전면허번호를 마스킹처리하지 않고 홈페이지에 등록하여 인터넷에 개인정보가 노출되었습니다.

▶ **경력사항**

강의실	기관명	강의시간
한국어 교원양성과정수료	[illegible]	2018.02.02 ~ 2018.04.02
한글 ITQ	[illegible]	2010.02.18 ~ 2010.11.20
개인정보보호 개론	[illegible]	2019.12.16 ~ 2019.12.31
1종 보통	제주지방경찰청	2004.01.03 ~ 제주[illegible]
품질관리 기초	[illegible]	2011.02.11 ~ 2011.03.08

[그림 16] 개인정보취급자의 게시물에 개인정보 노출된 사례

조치방법

상기 사례는 홈페이지 담당자가 신규 채용된 강사 경력정보를 홈페이지에 공개하면서 해당 정보를 마스킹 처리하지 않아 인터넷에 개인정보가 노출된 건입니다.

개인정보처리자는 개인정보가 포함된 게시물을 등록 시 마스킹 등 비식별 처리를 해야 합니다.

다. 개인정보가 포함된 게시글 및 댓글 게시

홈페이지 상에서 공지사항 및 게시판 등을 운영하는 개인정보처리자는 홈페이지관리자가 게시글 및 댓글에 개인정보를 기재할 경우 해당 게시글 및 댓글이 인터넷에 노출되지 않도록 관리·감독해야 합니다.

노출사례 ① – 게시글에 개인정보 노출

G지원센터는 지역 내 기업들에게 각종 지원정보 및 상담 서비스를 운영하고 있습니다. 또한 기업의 신기술에 대해서 지정하고 고시하는 역할도 하고 있습니다. G지원센터의 관리자가 B기업의 신기술 관련 내용을 고시하는 과정에서 신기술개발자의 개인정보(이름, 주민등록번호, 주소)를 노출하였습니다.

○ 신기술 보호기간 : 지정·고시일로부터 3년

나. [illegible] 공동접지기술 (기술)

○ 지정번호 : 제48호

○ 신기술개발자
- 회사명 : [illegible]
- 대표자 : [illegible]
- 법인(주민)등록번호 : 110111 [illegible], 750505-[illegible]
- 주 소 : 서울시 송파구 [illegible], 서울시 강남구 [illegible]

○ 신기술 내용 및 범위
- [illegible] 공동접지기술

○ 신기술 보호기간 : 지정·고시일로부터 3년

다음글	[illegible] 전원개발사업실시계획(변경)
이전글	[illegible] 품질경영 및 공산품안전관리법 시행령 전부개정령

[그림 17] 공지사항에 개인정보를 포함하여 게시

노출사례 ② – 이용자 문의 댓글에 개인정보 노출

외국인 교환 학생인 J씨는 학교 동아리 홈페이지에서 회원가입을 시도하였습니다. 하지만 해당 홈페이지에 회원 가입하려면 아이핀 또는 휴대폰인증 절차를 거쳐야하는데, 아이핀과 한국에서 개통한 휴대폰이 없는 J씨는 같은 과 친구를 통해 외국인 등록번호로 가입할 수 있는지 홈페이지 게시판에 문의하였습니다. 홈페이지 담당자가 문의 내용 답변으로 외국인 등록번호를 입력하면서 해당 개인정보가 노출 되었습니다.

[그림 18] 홈페이지관리자의 댓글에 개인정보 노출

조치방법

상기 두 사례는 홈페이지 담당자가 공지사항에 신기술 고시 및 정보주체의 민원을 해결하는 과정에서 홈페이지 담당자 부주의로 개인정보가 노출된 건입니다.

개인정보처리자는 홈페이지관리자가 게시글 및 댓글 작성 시 ▲마스킹 등의 방법을 통해 최소한의 개인정보를 기재 ▲부득이 개인정보를 적시해야 하는 경우 해당 게시글 및 댓글을 비공개로 전환할 수 있도록 관리해야 합니다.

[그림 19] 게시판을 비공개 게시판으로 운영

라. 개인정보가 포함된 첨부파일 게시

개인정보처리자는 비공개 게시판에 첨부파일을 게시할 수 있도록 안내해야 합니다.

특히 엑셀(Excel) 파일은 일정한 서식(행과 열)에 대량 정보를 저장하도록 고안되어 암호화를 하지 않고 공개 시 대량 노출로 이어질 가능성이 매우 높아 각별한 주의가 필요합니다.

첨부 파일 종류에 따른 개인정보 노출 유형은 다음 [표 1]와 같습니다.

[표 1] 엑셀 및 문서, 이미지 파일에 의한 노출 유형

구분	노출 유형
엑셀 파일에 의한 노출	[숨기기] 기능에 의해 개인정보가 노출
	시트보호기능으로 내용을 볼 수 없다고 오인하여 개인정보가 노출
	함수 치환 후 원본 내용 미삭제로 인해 개인정보가 노출
	[메모] 기능으로 개인정보가 노출
	배경색과 같은 글자색으로 작성하여 개인정보가 노출
문서 파일에 의한 노출	문서 파일에 개인정보가 노출
이미지 파일에 의한 노출	이미지 파일(JPG, PNG 등)에 개인정보가 노출
	이미지 형식(PDF 등)에 개인정보가 노출

노출사례 ① – 엑셀파일에 의한 개인정보 노출

A시는 대표홈페이지 내 정보공개 게시판을 통해 법률에 따라 공개 의무가 있는 업무관련 자료를 업로드 하고 있습니다. 종합민원실 담당인 B씨는 관내 「부동산중개업 등록 및 폐업 현황」 엑셀 파일을 공개 게시판에 업로드 하면서 개인정보를 마스킹 또는 삭제 처리하지 않아 다수의 개인정보(이름, 주민등록번호, 소재지, 연락처 등)가 노출되었습니다.

1515	여권 수수료 수납 및 송금현황	여권수수료 수납 및 송금현황(2017.12월)	종합민원실	2018-01-04
1514	토지거래 신고 및 허가 현황	토지거래 신고 및 허가현황(12월)	종합민원실	2018-01-04
1513	청소대행업체 수거량 및 대행료	청소대행업체 수거량 및 대행료(2017년 12월)	종합민원실	2018-01-03
1512	공인중개사법 위반업소 지도점검 결과	공인중개사법 위반업소 지도점검(2017년 4분기)	종합민원실	2018-01-02
1511	부동산중개업 등록 및 폐업 현황	부동산중개업 등록 및 폐업현황(2017년 4분기)	종합민원실	2018-01-02

부동산중개업 등록 및 폐업현황(2017년

홈 삽입 페이지 레이아웃 수식 데이터 검토 보기 어떤 작업을 원하시나요?

제한된 보기 주의하세요—인터넷에서 가져온 파일에는 바이러스가 있을 수 있습니다. 편집하지 않는다면 제한된 보기에서 여는 것이 안전합니다. 편집 사용(E)

주민등록

A	B	C	D	E	F	G	H	I
등록번호	대표	상호	소재지	주민등록번호	구분	폐업처리일자	폐업사유	연락처
[redacted]	이[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/1/4	개인사정	01[redacted]
[redacted]	이[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/1/9	개인사정	01[redacted]
[redacted]	정[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/1/19	개인사정	0[redacted]
[redacted]	유[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/2/6	개인사정	01[redacted]
[redacted]	허[redacted]	[redacted]동산[redacted]소	[redacted]	[redacted]	중계사	17/2/20	개인사정	01[redacted]
[redacted]	김[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/2/20	개인사정	01[redacted]
[redacted]	손[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/2/28	개인사정	01[redacted]
[redacted]	정[redacted]	[redacted]사사무소	[redacted]	[redacted]	중계사	17/3/9	개인사정	01[redacted]
[redacted]	엄[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/3/16	개인사정	01[redacted]
[redacted]	정[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/3/22	개인사정	01[redacted]
[redacted]	이[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/3/23	개인사정	01[redacted]
[redacted]	박[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/4/3	개인사정	0[redacted]
[redacted]	최[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/4/19	개인사정	01[redacted]
[redacted]	김[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/4/25	개인사정	01[redacted]
[redacted]	이[redacted]	[redacted]사무소	[redacted]	[redacted]	중계사	17/4/28	개인사정	01[redacted]

[그림 20] 엑셀파일에 의한 개인정보 노출 사례

노출사례 ② – 문서파일(HWP, DOC 등)을 통한 개인정보 노출

A복지관은 65세 이상 연장자를 대상으로 문화예술교육을 지원하고 있습니다. 분기별로 온·오프라인을 통해 신청자 접수를 받아, 참여자 명단을 홈페이지를 통해 공개하고 있습니다. 담당자 B씨는 2/4분기 교육 참여자 명단이 포함된 문서파일을 개인정보 마스킹하지 않고 공지사항 게시판에 업로드하여 해당 개인정보(성명, 주민등록번호, 연락처)가 노출되었습니다.

[그림 21] 문서파일에 의한 개인정보 노출 사례

노출사례 ③ – 이미지 파일(JPG, GIF, BMP, PNG, PDF 등)을 통한 개인정보 노출

해외 가족여행 계획을 세운 A씨는 B여행사를 통해 항공권과 숙소를 예약했습니다. 함께 가고 싶다는 조카의 부탁에 A씨는 예약인원 추가를 위해 조카의 여권사본(스캔본)을 여행사 담당자에게 메일로 보냈습니다. 하지만 업무담당자가 예약자 확인을 위해 홈페이지 공개 게시판에 조카의 여권사본 이미지 파일을 등록하면서 해당 개인정보(이름, 여권번호, 생년월일 등)가 노출되었습니다.

[그림 22] 이미지 파일에 의한 개인정보 노출 사례

조치방법

상기 사례는 홈페이지관리자가 법령 등에 정한 업무를 수행하면서 혹은 민원인 응대 과정에서 개인정보가 포함된 파일을 업로드하면서 해당 개인정보가 노출된 경우입니다.

개인정보처리자는 홈페이지관리자가 첨부파일 업로드 시 ▲첨부파일 내 개인정보 마스킹 ▲첨부파일이 공개되지 않도록 접근 제어 등의 조치를 취해 포함된 개인정보가 노출되지

않도록 관리·감독해야 합니다.

홈페이지관리자는 첨부파일 업로드 전에 해당 파일 내 개인정보가 존재하는지 확인해야 하며, 공개된 게시판에 첨부파일을 업로드해야하는 경우 마스킹 처리 등 비식별 처리해야 합니다.

특히 엑셀이나 한글 및 텍스트 기반의 PDF파일은 검색 기능을 통해 개인정보가 포함되어 있는지 확인해야 합니다. 이미지형 PDF 파일의 경우 PDF파일 생성 전 개인정보가 포함되어 있을 경우 해당 개인정보를 마스킹 처리하여 PDF파일로 변환하여야 합니다.

[그림 23] 이미지 마스킹 처리 예시

이미지 형식(JPG, PNG, GIF 등)의 첨부파일이 노출되었을 경우에는 해당 게시글을 비공개로 전환한 후에 첨부파일을 먼저 삭제하고, 이미지를 편집할 수 있는 소프트웨어(그림판 등)를 사용하여 개인정보 부분을 마스킹 처리한 후 재등록하도록 합니다.

NOTE!

특히, 엑셀파일의 경우에는 다양한 부가기능을 통해 개인정보가 숨겨져 있는 경우가 있으니 '[여기서, 잠깐!] 개인정보 노출의 원인이 되는 엑셀 부가기능 알아두기'를 참고하시기 바랍니다.

1) 숨기기

엑셀의 [숨기기(H)]란 행/열 또는 sheet를 숨기기 처리하여 현재 화면에서 보이지 않게 처리하는 기능입니다. sheet 내에서 숨기고 싶은 행/열에 마우스 우클릭 시 나타나는 메뉴에서 [숨기기(H)] 클릭 시 해당 행/열이 숨김처리가 되고 숨김처리된 행/열은 보이지 않는 상태가 됩니다.

[그림 24] 숨기기 메뉴

[그림 25] 숨기기 기능 사용 후

숨기기 기능 사용 시 E열이 위 그림과 같이 열 자체가 보이지 않게 됩니다.

숨겨진 행/열은 [숨기기 취소(U)] 기능을 이용해 나타나게 할 수 있습니다. 숨겨진 열인 E열의 양옆에 있는 열(D~F)을 드래그한 후 우클릭 시 나타나는 메뉴에서 [숨기기 취소(U)]를 통해 숨김처리된 열을 숨김 취소할 수 있습니다.

[그림 26] 숨기기 취소 메뉴

[그림 27] 숨기기 취소 기능 사용 후

개인정보가 포함된 행/열 또는 Sheet를 [숨기기] 처리한 파일을 열었을 때에는 개인정보가 바로 보이지 않지만 행/열 또는 Sheet [숨기기 취소]를 할 경우 개인정보가 나타나기 때문에 개인정보 노출이 발생하게 됩니다.

노출사례

엑셀의 숨기기 기능을 잘못 활용하여 개인정보 노출이 발생하는 경우입니다. 개인정보가 있는 셀을 삭제하지 않고 행/열 또는 sheet를 [숨기기] 처리 후 업로드 하여 현재 보이지 않는 상태이지만 숨겨진 정보는 삭제된 것이 아니라 그대로 남아있게 되어 개인정보 노출이 발생합니다.

[그림 28] 숨기기 기능을 통한 개인정보 노출 예시

조치방법

홈페이지관리자가 첨부파일 업로드 전 엑셀 파일에서 행/열 또는 Sheet [숨기기 취소] 기능으로 숨겨진 개인정보가 있는지 확인 후 개인정보가 존재할 경우 삭제하거나 식별할 수 없도록 마스킹 처리 후 업로드 하여야 합니다.

[그림 29] 숨기기 처리된 개인정보 확인

2) 시트보호

엑셀의 [시트보호]란 특정 워크시트에 대해 접근권한을 설정하여, 접근권한이 없는 자의 데이터 수정을 방지하는 기능입니다. (MS OFFICE 2016 버전의 경우) 파일 → 정보 메뉴 → 통합문서 보호 → 현재 시트 보호(P) 메뉴를 클릭 시 사용할 수 있습니다.

[그림 30] 시트보호 메뉴

[그림 31] 시트보호 설정

노출예시

일부 사용자는 엑셀 내 개인정보가 포함된 경우 문서 전체를 암호화하는 대신, 해당 행 또는 열을 숨기기 처리하고 숨기기 취소가 안 되도록 시트보호기능을 설정합니다. 하지만 시트보호기능을 설정하더라도 데이터가 암호화되지 않으며, 찾기 및 바꾸기 [Ctrl+F]를 통해 데이터 검색이 가능하므로 개인정보가 노출되게 됩니다.

[그림 32] 시트보호로 개인정보가 보호되지 않는 예시

조치방법

상기 사례는 파일 사용자가 시트보호 비밀번호를 모를 경우 포함된 개인정보 확인이 불가능합니다. 하지만 찾기 및 바꾸기[Ctrl+F], 파일 검색 프로그램이나 검색엔진에 의해 보호된 개인정보가 노출될 수 있으므로, 이와 같이 시트보호기능이 적용된 시트에는 개인정보를 포함해서는 안 됩니다.

3) 치환 함수

엑셀 함수를 이용하면 특정 명령어를 사용하여 방대한 양의 작업을 손쉽게 처리할 수 있습니다. 그 중 REPLACE, SUBSTITUTE 함수는 텍스트 내의 문자를 바꾸는 기능으로 개인정보(전화번호, 주민등록번호, 운전면허번호 등)를 마스킹 처리할 때 사용할 수 있습니다.

함수명	사용함수	기존값	결과값
REPLACE	=REPLACE(F3,9,6,"*******")	801212-1234567	801212-1*******
SUBSTITUTE	=SUBSTITUTE(F4,"234567","*******")	801212-1234567	801212-1*******

[그림 33] REPLACE, SUBSTITUTE 함수 사용 예시

해당 함수를 사용하여 개인정보를 마스킹할 경우 결과값은 마스킹 처리(******)되어 보이지만, 함수는 원본 데이터를 참조하여 마스킹처리하기 때문에 원본 데이터는 남아있게 됩니다. 결국 보기에는 마스킹 처리되었지만 실제로는 해당 정보가 엑셀 내 남아 있는 것입니다.

노출예시

개인정보가 포함된 셀을 REPLACE 등의 함수를 이용하여 마스킹 처리(D열)했지만 원본(C열)은 마스킹 되지 않고 남아있습니다. 엑셀 내 함수를 이용하여 마스킹 처리 후 원본을 삭제하지 않아 개인정보가 노출되었습니다.

NO	성명	주민등록번호	주민등록번호	체납건수	체납액
1	조*일	740912-1	740912-1******	10	1,000,000
2	김*이	661002-1	661002-1******	13	1,300,000
3	김*삼	500609-2	500609-2******	39	3,900,000
4	이*사	730730-2	730730-2******	14	1,400,000
5	박*오	401213-2	401213-2******	14	1,400,000
6	권*육	500506-1	500506-1******	18	1,800,000
7	고*칠	480607-1	480607-1******	22	2,200,000

[그림 34] 함수 치환 기능을 통한 개인정보 노출 예시

조치방법

첨부파일 업로드 시 함수 치환 기능을 사용하여 개인정보를 마스킹 처리하였지만, 이 경우 마스킹 처리를 위한 원본 자료가 함께 존재하므로 원본 자료를 반드시 삭제해야 합니다.

NO	성명	주민등록번호	체납건수	체납액
1	조*일	740912-1******	10	1,000,000
2	김*이	661002-1******	13	1,300,000
3	김*삼	500609-2******	39	3,900,000
4	이*사	730730-2******	14	1,400,000
5	박*오	401213-2******	14	1,400,000
6	권*육	500506-1******	18	1,800,000
7	고*칠	480607-1******	22	2,200,000

[그림 35] 함수 치환 후 원본자료 삭제

4) 메모

엑셀의 [메모]는 개별 셀에 주석을 추가하여 추가 설명 등을 제공할 수 있는 기능이며 메모가 있는 셀의 모서리에는 빨간색 표식이 나타납니다. 메모가 있는 셀에 마우스를 놓으면 해당 메모가 표시됩니다. 메모 기능의 설정은 메모를 추가하고 싶은 셀에 마우스 우클릭 후 나타나는 메뉴에서 [메모 삽입(M)] 메뉴를 클릭하면 메모가 추가되고 메모 내용을 작성할 수 있게 됩니다.

[그림 36] 메모 삽입 메뉴

[그림 37] 메모 삽입 후 화면

노출예시

마스킹 처리된 개인정보를 업무상 편의를 위해 [메모]에 개인정보를 작성한 경우입니다. [메모]에 개인정보를 작성해놓을 경우 평소에는 보이지 않다가 마우스 커서를 올려놓게 되면 메모에 작성한 내용이 보이게 됩니다. 메모에 작성된 주민등록번호를 삭제하지 않고 업로드 하게 되어 개인정보가 노출되었습니다.

NO	성명	주민등록번호	체납건수	체납액
1	조*일	740912-1******		1,000,000
2	김*이	661002-1******		1,300,000
3	김*삼	500609-2******		3,900,000
4	이*사	730730-2******	14	1,400,000
5	박*오	401213-2******	14	1,400,000
6	권*육	500506-1******	18	1,800,000
7	고*칠	480607-1******	22	2,200,000

메모 :
주민등록번호 :
740912-1

[그림 38] 메모 기능을 통한 개인정보 노출 예시

조치방법

숨겨진 메모는 메모 숨기기 취소 기능을 통해 언제든지 내용을 다시 확인할 수 있으므로 개인정보가 포함되어 있는 메모는 삭제해야 합니다.

5) 글자색과 배경색이 같은 경우

파일 내 개인정보의 글자색과 배경색이 같아서 개인정보가 없는 것 처럼 보이는 경우입니다. 육안으로는 보이지 않지만, 검색이나 드래그를 통해 없는 것처럼 보이는 글자들을 확인할 수 있습니다.

노출예시

다음은 주민등록번호를 배경색과 같은 글자색(흰색)으로 작성하여, 웹사이트 이용자가 육안으로 확인할 수 없었던 경우입니다.

NO	성명	주민등록번호	체납건수	체납액
1	조*일	740912-1******	10	1,000,000
2	김*이	661002-1******	13	1,300,000
3	김*삼	500609-2******	39	3,900,000
4	이*사	730730-2******	14	1,400,000
5	박*오	401213-2******	14	1,400,000
6	권*육	500506-1******	18	1,800,000
7	고*칠	480607-1******	22	2,200,000

[그림 39] 배경색과 같은 색상으로 글자색을 지정하여 개인정보가 노출된 예시

조치방법

상기 사례는 육안으로 확인이 불가능합니다. 엑셀 파일을 홈페이지에 업로드하는 경우에는, 반드시 전체 셀을 선택 후 셀 배경색을 채우기 없음 및 글자색 자동으로 설정해서 혹시 숨겨진 개인정보가 없는지 확인해야 합니다.

[그림 40] 셀 배경색 채우기 없음 설정

[그림 41] 글자색 자동 설정

6) OLE 객체

OLE(Object Linking and Embedding)는 마이크로소프트에서 개발한 '통합문서'의 표준을 뜻합니다. 통합문서는 서로 다른 응용프로그램에서 고유의 형태를 유지한 채 다른 프로그램에서 불러와 삽입하여 쓸 수 있는 기능입니다.

노출예시

MS WORD 프로그램을 이용해 보고서를 작성 중 엑셀에서 만든 차트를 삽입하여 사용하였습니다. 하지만 OLE 객체 연결로 인해 MS WORD의 차트에서 [데이터 편집] 클릭 시 차트를 만들 때 사용한 엑셀 파일이 열리게 되었고, 해당 엑셀에 함께 저장되어 있던 개인정보가 노출되었습니다.

[그림 42] OLE 객체에 의한 개인정보 노출 예시

조치방법

OLE 객체는 서로 다른 응용프로그램에서 작성한 자료(차트, 이미지 등)를 링크(연결)를 통해 해당 응용프로그램에서 사용하는 기능으로 다른 프로그램에서 작성한

내용이 함께 보여 질 수 있으니 외부 링크(파일 연결)를 해제하고 사용해야 합니다. MS WORD의 경우 [파일 → 정보 → 파일 연결 편집 → 연결 끊기] 기능을 통해 다른 파일의 연결을 해제할 수 있습니다.

[그림 43] OLE 객체에 의한 개인정보 노출 사례 조치방법-1

[그림 44] OLE 객체에 의한 개인정보 노출 사례 조치방법-2

2. 이용자 부주의에 의한 개인정보 노출

가. 개인정보가 포함된 게시글 및 댓글 작성

홈페이지 상에서 공지사항 및 게시판 등을 운영하는 개인정보처리자는 홈페이지 이용자가 게시글 및 댓글에 개인정보를 기재할 경우 해당 게시글 및 댓글이 인터넷에 노출되지 않도록 관리·감독해야 합니다.

노출사례 ① – 게시글에 개인정보 노출

신혼여행을 계획 중인 A씨는 그동안 모아왔던 마일리지로 좌석 업그레이드 서비스 신청을 위해 여권번호가 포함된 문의 글을 항공사 고객센터 게시판에 공개글로 작성하면서 해당 개인정보가 노출되었습니다.

[항공권 구매기록] 문의

작성자 [redacted]

안녕하세요.

항공사 마일리지 적립을 위하여 다음과 같은 사항 요청 드립니다.

* 탑승자명 : [redacted]
* 여권번호 : [redacted]
* 요청사항 : 2015년~2016년의 항공권 구매기록 및 티켓번호
* 연락처 : 010-[redacted]

[그림 45] 홈페이지 이용자의 게시글에 개인정보가 노출된 사례

노출사례 ② – 이용자 문의 댓글에 개인정보 노출

개인사업자인 A씨는 P사 홈페이지에서 펜, 수첩 등 판촉물을 대량 구매하면서 세금계산서 발급을 요청하였습니다. 뒤늦게 세금계산서가 발급되지 않았다는 사실을 알게 된 A씨는 P사 홈페이지에 댓글로 세금계산서 발급을 요청하면서 해당 개인정보(성명, 주민등록번호, 연락처)가 노출되었습니다.

[그림 46] 댓글에 의한 개인정보 노출

조치방법

상기 두 사례는 홈페이지 이용자가 게시판 및 댓글을 통해 문의하는 과정에서 홈페이지 이용자의 부주의로 개인정보가 노출된 건입니다.

개인정보처리자는 홈페이지 운영 중 이용자 부주의에 의한 개인정보 노출이 발생하면 ▲게시물 비공개 전환 ▲게시물 삭제 ▲개인정보를 입력하지 않도록 안내 ▲비공개 게시판 운영 등의 조치를 취해 개인정보가 노출되지 않도록 관리·감독해야 합니다.

홈페이지 이용자가 작성한 게시물에 개인정보가 포함되어 있을 경우, 게시물을 비공개 전환하여 개인정보가 노출되지 않도록 임시조치하고, 해당 게시물을 삭제하거나 개인정보를 123456-1******와 같이 마스킹 처리 한 후 재등록해야 합니다.

이 후 게시글 작성 시 작성 글에 개인정보를 포함하지 않도록 공지사항 또는 안내 문구를 이용하여 작성자에게 안내해야 합니다.

[그림 47] 게시글 작성 시 개인정보 노출에 대한 경고문구 삽입(예시)

또한 이용자의 부주의에 의해 개인정보 노출이 재발하지 않게 게시글 작성 시 작성자와 홈페이지 담당자만 확인할 수 있도록 비공개 설정할 수 있는 기능을 추가하여 게시판을 비공개 게시판으로 운영해야 합니다.

[그림 48] 비공개 게시판 운영(예시)

나. 개인정보가 포함된 첨부파일 게시

첨부파일 등록 기능이 포함된 홈페이지를 운영하는 개인정보처리자는 홈페이지 이용자가 개인정보가 포함된 첨부파일을 등록 시 비공개 게시판에 첨부파일을 게시할 수 있도록 관리해야 합니다.

특히 엑셀(Excel) 파일은 일정한 서식(행과 열)에 대량 정보를 저장하도록 고안되어 암호화를 하지 않고 공개 시 대량 노출로 이어질 가능성이 매우 높아 각별한 주의가 필요합니다.

노출사례 ① – 문서파일(HWP, DOC 등)을 통한 개인정보 노출

A협회는 수도권 대기환경개선에 관한 특별법 제27조(노후차량의 조기폐차 지원 등)에 따라 정상운행이 가능한 오래된 경유자동차를 조기 폐차할 경우 보조금을 지원하는 사업을 운영하고 있습니다. 이 사업을 알게 된 C씨는 노후차량 조기폐차 보조금을 지급받기 위해 "조기폐차 보조금 지급청구서"를 작성하여 A협회 홈페이지에 게시하였습니다. 하지만 개인정보(성명, 주민등록번호, 주소, 전화번호 등)가 기재된 지급청구서를 공개된 게시판에 업로드하게 되어 개인정보가 노출되었습니다.

확인번호	조기폐차 보조금 지급청구서			
소유자	성 명		주민등록번호	
	주 소			
	전화번호		FAX	
신 청 자동차	자동차번호		차대번호	
	자동차제원			
	등록일자(차령)			
	주행거리			
	보조금신청금액			
폐차 관련	말소 일자			
	신차 구매계획			

위와 같이 노후차량을 조기폐차한 후 해당내역을 신고하오니, 조기폐차에 따른 보조금을 지급하여 주시기 바랍니다.

2018 년 06 월 07 일

신청자 : (인)

시장(지사) 귀하

※ 첨부서류

1. 자동차 말소 등록증(원본 또는 사본)
2. 자동차 소유자의 보조금 지급요청 통장 사본
3. 조기폐차 대상차량 확인서

[그림 49] 신청서 내 개인정보가 작성된 사례

노출사례 ② – 이미지 파일(JPG, GIF, BMP, PNG, PDF 등)을 통한 개인정보 노출

주택재개발 사업을 진행 중인 A구청은 지역 주민 의견 수렴을 위해 홈페이지 내 민원 게시판을 운영하였습니다. 재개발사업 지역에서 상가를 운영하고 있는 C씨가 A구청에 민원을 제기하는 과정에서 상가·점포 임대차계약서를 공개 게시판에 업로드하여 개인정보(성명, 주민등록번호, 전화번호, 주소 등)가 노출되었습니다.

[그림 50] 이미지형 PDF 파일에 의한 노출 사례

조치방법

상기 두 사례는 홈페이지 이용자의 부주의로 인해 개인정보가 포함된 첨부파일을 업로드하면서 해당 개인정보가 노출된 경우입니다.

개인정보처리자는 홈페이지 운영 중 이용자 부주의에 의한 개인정보 노출이 발생하면 ▲게시물 비공개 전환 ▲게시물 삭제 ▲개인정보를 입력하지 않도록 안내 ▲비공개 게시판 운영 등의 조치를 취해 개인정보가 노출되지 않도록 관리·감독해야 합니다.

이용자가 업로드 한 첨부파일에 의해 개인정보 노출이 발생하면 홈페이지관리자는 해당 작성글을 삭제 후 이용자에게 개인정보가 포함되어 게시글을 삭제한 내용을 안내하거나, 해당 게시글을 신속히 비공개 처리하여 작성자와 홈페이지관리자만 열람할 수 있도록 조치해야 합니다.

추가 조치로 공개 게시판에 글 작성 시 개인정보를 포함하지 않도록 공지사항 또는 안내 문구를 통해 작성자에게 안내해야 합니다. 업무상 개인정보 입력이 불가피한 경우엔 해당 게시판을 비공개 게시판으로 운영하여 작성자와 개인정보처리자만 글을 확인할 수 있도록 조치해야 합니다.

[그림 51] 게시판 글 작성 시 안내 문구 및 비공개 설정 기능

3. 홈페이지 설계 및 개발 오류에 의한 노출

가. 홈페이지 접속경로(URL) 관련 오류

1) URL 내에 개인정보 포함

웹 전송방식은 변수명, 변수값이 URL에 보이는 유무에 따라 GET 방식과 POST 방식으로 나뉩니다. POST 방식은 변수명, 변수값이 URL에 노출되지 않아 보안에 강하지만, 성능 및 외부 링크 시 추가 개발 등의 이유로 홈페이지 개발자는 경우

(게시판 번호 등 개인정보가 전달되지 않는 경우)에 따라 웹 전송방식으로 GET 방식을 사용합니다. 개인정보처리자는 개발자가 POST 방식을 사용할 수 있도록 안내하고 부득이하게 GET 방식을 이용할 경우 URL내 개인정보가 포함되지 않도록 관리·감독해야 합니다.

노출사례 ① – 홈페이지 접속경로(URL)에 개인정보 포함

H고등학교는 홈페이지를 통해 이력서 관리 서비스를 학생들에게 제공하고 있습니다. 해당 시스템은 이력서 내 사진파일 이름을 주민등록번호로 저장하도록 개발되었습니다. 학생들이 자신의 사진을 열람하거나, 다운로드 받을 때 사진 파일명이 URL에 사용되면서, 주민등록번호가 노출되었습니다.

[그림 52] URL에 주민등록번호가 노출된 사례

2) URL 내 포함된 변수값을 조작하여 타인의 개인정보 조회

통상적으로 게시판에서 게시물 조회시 GET 방식을 이용하는데(게시물 내용 조회를 위한 게시물 번호를 URL을 통해 웹 서버로 전달) 설계 및 개발 오류로 변수값 조작을 통해 타인의 비공개된 게시물까지 조회 가능하게 되어 문제가 됩니다.

따라서 웹 전송방식으로 GET 방식을 이용하는 개인정보처리자는 변수값 조작을 통해

타인의 정보가 조회되지 않도록 관리·감독해야 합니다.

노출사례 ② – 접속경로(URL) 변경을 통한 타인의 개인정보 접근

대학생인 K씨는 이메일이 변경되어 해당 정보를 수정하기 위해 학사관리시스템에 접속하였습니다. K씨는 홈페이지 URL 내 파라미터로 자신 학번이 사용되는 것을 확인하고, 호기심에 친구의 학번을 입력하자 친구의 개인정보(이메일, 주소, 연락처 등)를 수정할 수 있는 페이지가 출력되었습니다.

[그림 53] URL값 변경 시 다른 회원의 정보가 노출된 사례

조치방법

상기 사례는 홈페이지 설계 및 개발 오류로 ① 홈페이지 전송방식으로 GET 방식 사용 ② URL 내 파라미터로 개인정보(주민등록번호 등)를 사용하여 개인정보 노출이 발생한 건입니다.

홈페이지 접속경로(URL) 관련 오류에 의한 개인정보 노출이 발생하면 ▲ 이용자 자신의 정보만 조회 가능하도록 접근제어 ▲ 회원 구분 값 변경 ▲ 홈페이지 설계 변경(GET 방식에서 POST 방식으로) 등을 통해 개인정보 노출을 방지해야 합니다.

접근권한 관리가 미흡한 경우 가입된 이용자들의 개인정보가 노출되어 해당 정보가 악용되는 피해가 발생할 수 있습니다. 이를 위해 회원정보가 조회 가능한 페이지는 이용자 본인만 확인할 수 있도록 인증 정보 확인 등의 방법으로 접근 통제해야 합니다.

또한, 회원 구분 값으로 주민등록번호 등 개인정보를 이용해서는 안되며, 웹브라우저 주소 표시줄에 파라미터 값이 보이지 않도록 GET 방식 보다는 POST 방식을 사용해야 합니다.

[그림 54] URL에 개인정보가 노출된 경우 조치 방법

여기서, 잠깐!

GET 방식과 POST 방식 알아보기

■ GET 방식

Form 태그 method 속성 값으로 GET을 지정할 경우 변수명, 변수값이 URL 주소에 노출됩니다.

[그림 55] GET 방식

URL과 파라미터를 구분하기 위해 "?"를 구분자로 쓰며, 파라미터가 여러 개 일 경우 "&"를 각 파라미터의 구분자로 사용합니다.

구분자 "?" 뒤에 오는 값이 파라미터 값입니다.

[그림 56] GET 방식 파라미터 값

URL 자체에 데이터를 포함시키기 때문에 URL 자체가 하나의 긴 문자열입니다. 또한 HTTP 헤더에서 GET 방식이라고 HTTP 메소드 부분에 표시됩니다.

[그림 57] GET 방식 HTTP 헤더

■ POST 방식

Form 태그 method 속성 값으로 POST를 지정할 경우 변수명, 변수값이 URL 주소에 노출되지 않습니다. GET 방식과는 다르게 길이의 제한이 없으며, 보안을 지킬 수 있다는 이점이 있습니다. 아래 그림과 같이 HTTP 헤더에서 POST 방식이라고 HTTP 메소드 부분에 표시됩니다.

```
Hypertext Transfer Protocol
  POST /status HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /status HTTP/1.1\r\n]
      [POST /status HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: POST
    Request URI: /status
    Request Version: HTTP/1.1
```

[그림 58] POST 방식 HTTP 헤더

나. 홈페이지 소스코드 보안설정 미흡

정적홈페이지와 달리 동적홈페이지는 홈페이지 조회 시 매번 페이지를 새로 생성합니다. 홈페이지 조회시 WAS서버는 DB서버로부터 정보를 가져와 소스코드를 생성하고, 해당 소스코드가 웹브라우저를 통해 이용자에게 보여집니다. 문제는 개발자가 화면에서 보이는 것보다 더 많은 정보를 DB에서 가져오도록 개발하였다면, 화면에서 보이지 않는 개인정보 등이 소스코드에 포함됩니다. 따라서 개발 단계에서부터 불필요한 개인정보가 소스코드에 포함되지 않도록 주의하고, 부득이 개인정보가 소스코드에 포함되어야 한다면 반드시 필요한 정보(화면에서 보여지는 정보)만 소스코드 내에 포함되도록 개발해야 합니다.

노출사례

노트북 중고 판매업체인 A사는 제품 홍보 등을 위해 홈페이지 내 정보나눔방을 운영하고 있습니다. A사 직원인 J씨는 정보 나눔방 게시글에 노트북 특가 이벤트 관련 글을

게재하였습니다. 해당 게시글에는 개인정보가 표시되지 않지만, 홈페이지 소스코드 보안설정 미흡으로 해당 화면에서 마우스 오른쪽 클릭 후 [소스 보기]를 했을 때 작성자의 개인정보(주민등록번호)가 표시(노출)됩니다.

[그림 59] 소스 보기에서 개인정보가 노출된 사례

조치방법

상기 사례는 홈페이지 소스코드 보안설정 미흡으로 [마우스 우클릭] 〉 [소스 보기] 시 작성자의 개인정보가 노출 된 건입니다.

홈페이지 소스보기에 의한 개인정보 노출이 발생하면 ▲노출 페이지에 대한 접근제어 ▲회원 구분 값 변경(개인정보가 포함되지 않은 식별자 이용)에 의한 개인정보 노출을 방지해야 합니다.

[소스 보기]를 통해 홈페이지 소스코드에 개인정보가 포함되지 않도록 회원 식별 값을 개인정보가 아닌 회원번호 등으로 변경해야 합니다.

[그림 60] 웹사이트 소스코드 내에 회원 구분 값 변경

개발자는 개인정보가 포함된 식별자가 홈페이지 소스코드 내에 포함되지 않도록 주의해야 합니다.

다. 임시 저장 페이지 미삭제

이용자 편의를 위해 임시 저장 페이지를 운영하는 개인정보처리자는 이용자 로그아웃 시 이용자가 임시 저장했던 내용들을 모두 삭제해야합니다. 만일 삭제하지 않고

일정기간 보관해야 한다면, 임시 저장했던 내용이 로그인 등 인증없이 인터넷에서 접근되지 않도록 관리해야 합니다.

노출사례

K여행사는 홈페이지 내 고객 편의를 위해 고객 메모용으로 임시저장페이지 기능을 제공하였습니다. K여행사 회원인 A씨는 겨울 휴가로 가족 여행을 계획하면서, 여행사 홈페이지 내 임시보관함에 가족 여권번호를 입력하였습니다. K여행사 임시보관함이 인터넷에 공개되면서, 해당 개인정보가 노출되었습니다.

[그림 61] 임시보관함에 저장된 게시글 노출 사례

조치방법

상기 사례는 이용자 편의를 위해 제공된 임시저장페이지에 포함된 개인정보가 노출된 건입니다.

개인정보처리자는 임시 저장 페이지에서 개인정보가 노출되지 않도록 하기 위해서 ▲게시글 작성 완료 및 작성 취소 시 저장된 임시 페이지를 바로 삭제 ▲일정기간이 경과된 임시저장 페이지는 자동으로 삭제될 수 있도록 조치해야 합니다.

라. 디렉터리 리스팅 보안설정 미흡

디렉터리 리스팅이란 보안 취약점 중 하나로 웹 서버 설정 미숙 등을 이유로 웹 브라우저를 통해 웹 서버의 디렉터리, 파일 목록이 노출되고, 열람 및 다운로드가 가능하게 되는 것을 말합니다. 개인정보처리자는 이러한 디렉터리 리스팅이 발생하지 않도록 사용하고 있는 웹 서버 등의 설정을 점검해야 합니다.

특히 해당 유형에서는 웹 서버 내 모든 파일이 인터넷에 무방비로 노출 되어 개인정보 유출 사고로 이어질 수 있으므로 각별한 주의가 필요합니다.

노출사례

인권 보호를 위해 만들어진 단체인 A협회는 직장인들을 대상으로 회원제 커뮤니티를 운영하고 있습니다. 직장인 P씨는 회사의 내 성희롱 문제를 상담하고자 포털사이트를 통해 A협회 홈페이지로 접속하였습니다. 하지만 해당 사이트에서 디렉터리 리스팅 차단을 설정하지 않아 홈페이지 메인화면 대신 디렉터리 리스팅 화면이 출력되어, 웹 서버 내 회원 정보가 노출되었습니다.

조치방법

상기 사례는 홈페이지 설계 오류 중 디렉터리 리스팅 취약점에 의해 개인정보 노출이 발생한 건입니다.

디렉터리 리스팅에 의한 개인정보 노출이 발생하면 ▲접근제어 설정 ▲디렉터리 설정 변경 등 해당 디렉터리를 외부에서 읽지 못하도록 관리해야 합니다. 웹 서버별 디렉터리 리스팅 취약점을 해결하는 방법은 다음과 같습니다

1) Apache 1.x, 2.x : httpd.conf 파일에서 indexes 문자열 제거

```
<Directory "/user/local/server/apache/htdocs">
        Options Indexes  삭제
</Directory>
```

2) Tomcat : web.xml 파일에서 〈param-value〉 태그 false 로 설정변경

```
<Init-param>
  <param-name>listings</param-name>
  <param-value>false</param-value>
</init-param>
```

3) Nginx : Nginx.conf 파일에서 autoindex 설정을 off 로 변경

```
Location  {
    Autoindex off;
}
```

4) 윈도우즈 IIS(Internet Information Service) 환경

① IIS 6.x 이하 : 제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 웹사이트의 속성에서 디렉터리 검색 항목을 비활성화

[그림 62] IIS 6.x 이하에서 디렉터리 리스팅 방지 설정

② IIS 7.x : 제어판 → 관리도구 → 인터넷 서비스 관리자 → 기본 웹사이트 홈 → 디렉터리 검색을 더블클릭 후 우측 작업창에서 사용 해제

③ IIS 8.x : 제어판 → 시스템 및 보안 → 관리도구 → IIS(인터넷 정보서비스) 관리자 → 사이트 → 기본 웹사이트 홈 → 디렉터리 검색을 더블클릭 후 우측 작업창에서 사용 해제

[그림 63] IIS 7.x 및 8.x에서 디렉터리 리스팅 방지 설정

4. 검색엔진을 통한 개인정보 2차 노출

가. 검색엔진의 이해

검색엔진이란 인터넷 상에서 자료를 쉽게 찾을 수 있도록 검색사이트가 구축한 시스템입니다. 검색엔진은 정보수집·정보가공·정보제공의 세 가지 기능으로 구성되는데 정보수집은 크롤러, 정보가공은 인덱서, 정보제공은 사용자 인터페이스가 담당합니다. 검색엔진의 정보수집 단계에서 크롤러가 인터넷에 있는 웹사이트를 주기적으로 방문하여 각종 정보를 자동으로 수집하는데, 이 때 웹사이트의 일부 웹페이지가 검색엔진 내 일정기간 동안 보관됩니다. 가령 주민등록번호 등 개인정보를 포함한 웹페이지가 검색엔진에 수집될 경우 원 사이트에서 해당 웹페이지의 개인정보를 삭제 조치하더라도, 크롤러가 개인정보 삭제 조치 완료된 웹페이지를 재 수집하지 않는 이상

개인정보가 여전히 검색엔진에 검색될 수 있습니다. 따라서, 홈페이지에 개인정보가 잠시라도 업로드 된 경우에는 반드시 해당 노출 내용이 검색엔진에 의해 수집되었는지를 확인하고 검색엔진에 남아 있는 노출정보를 삭제해야 합니다.

노출사례

A협회는 화장품 제조사의 사업계획서 및 사업자등록증, 이력서 등을 관리하고 있습니다. A협회는 자체 개인정보 관리실태 점검 시 홈페이지 설계 상 오류로 직원 이력서가 노출된 사실을 인지하고 삭제 조치하였습니다. 하지만 삭제 조치된 직원 이력서가 검색엔진의 저장된 페이지에 남아있어, 이력서 내 개인정보가 검색엔진을 통해 2차 노출되었습니다.

[그림 64] 검색엔진을 통한 개인정보 2차 노출

나. 검색엔진별 개인정보 노출 조치방안

우선 기관 홈페이지 내 노출된 개인정보가 인터넷에 노출되지 않도록 조치완료 후, 혹시 모를 검색엔진을 통한 2차 노출을 방지하기 위해 검색사이트에서 노출된 페이지의 URL 또는 노출된 값으로 검색을 수행합니다. 검색 결과, 노출조치 완료된 웹페이지가

검색사이트 캐쉬 페이지에 저장된 경우, 검색사이트에서 제공하고 있는 웹마스터 도구 또는 고객센터를 통하여 해당 캐쉬 페이지를 삭제해야 합니다. 검색사이트별 캐쉬페이지 삭제 요청 웹사이트는 다음과 같습니다.

[표 2] 검색 사이트별 캐쉬페이지 삭제 요청 주소

검색사이트	명칭	삭제요청 주소
네이버(Naver)	삭제 문의 고객센터	https://help.naver.com/support/home.nhn
다음(Daum)	권리침해 신고센터	https://cs.daum.net/redbell/top.html
구글(Google)	오래된 컨텐츠 삭제	https://www.google.com/webmasters/tools/removals
빙(BING)	오래된 컨텐츠 삭제	https://www.bing.com/webmaster/help/bing-content-removal-tool-cb6c294d

1) 네이버

인터넷에 노출된 개인정보가 네이버 검색엔진에 의한 2차 노출된 것을 발견하면, 아래와 같은 절차로 네이버 고객센터에 방문하여 삭제 조치를 수행합니다.

[그림 65] 네이버 검색엔진 2차 노출 조치 절차

① 네이버 고객센터 방문

네이버 고객센터를 방문하여 신고센터 〉 유해 게시물 신고 메뉴를 클릭합니다.

[그림 66] 네이버 고객센터 방문

② 네이버 게시물 신고 접수

게시물 신고접수에서 신고하는 이유(개인정보 노출)을 선택합니다.

[그림 67] 신고접수 메뉴 선택 ‘개인정보 노출’

③ 노출되는 위치 선택

개인정보 노출이 발생한 게시물이 어디에서 노출되고 있는지 선택합니다.(네이버 검색결과)

[그림 68] 신고접수 메뉴 선택 '네이버 검색결과'

④ 검색 제외 요청하기

검색엔진에서 개인정보가 노출되는 게시물을 검색 제외하기 위해 '검색 제외 요청하기' 메뉴를 선택합니다.

[그림 69] 검색 제외 요청하기 메뉴 선택

⑤ 게시물의 작성자 선택

개인정보가 노출된 게시물의 작성자를 선택합니다.

[그림 70] 게시물의 작성자 선택

⑥ 게시물 상태 선택

검색 제외를 원하는 게시물의 상태를 선택합니다. 원본 게시물을 삭제 후 캐쉬페이지 삭제 요청을 하는 것이 좋으며, 원본 게시물을 삭제하지 않고 캐쉬페이지 삭제 시 추후 또 다시 캐쉬페이지로 노출될 수 있습니다.

[그림 71] 원본 게시물의 삭제여부 선택

⑦ 신청자 정보 입력 및 신청완료

마지막으로 이메일, 삭제할 게시물 URL, 검색 키워드, 검색결과 URL, 요청사유, 사유 선택, 개인정보 수집·동의 등 상세정보를 입력하여 캐쉬페이지 삭제 요청을 완료합니다.

[그림 72] 검색 제외를 위한 상세 정보 입력

2) 다음

인터넷에 노출된 개인정보가 다음 검색엔진에 의한 2차 노출된 것을 발견하면, 아래와 같은 절차로 다음 고객센터에 방문하여 삭제 조치를 수행합니다.

[그림 73] 다음 검색엔진 2차 노출 조치 절차

① 다음 고객센터 - '검색' 탭 접속

다음 검색엔진의 고객센터에 접속하여 '검색' 탭을 선택합니다.

[그림 74] 다음(DAUM) 고객센터 화면

② 검색결과 제외 선택

다음 검색엔진의 고객센터에 접속하여 '검색' 탭을 선택합니다.

[그림 75] 다음(DAUM) 고객센터 검색 탭에서 '검색결과 제외' 선택

③ 검색결과 제외 신청 선택

검색결과 제외 탭에서 '개인정보가 포함된 게시글이 검색되는데 삭제할 수 있나요?'의 내용 확인 시 Daum 고객센터 문의하기 링크를 통해 개인정보가 포함된 게시글 삭제 요청을 할 수 있습니다. 검색 URL, 키워드, 원문 URL, 원문게시물 제목, 삭제요청사유를 기입하여 삭제요청을 합니다.

[그림 76] 검색결과 제외 탭에서 '개인정보가 포함된 게시글 삭제에 대한 글 확인'

④ 제외신청 접수완료

필수항목(검색 URL, 키워드, 원문 URL, 원문게시물 제목, 삭제요청사유)을 작성하여 접수 시 개인정보 노출에 대한 삭제 요청이 접수되어 처리됩니다.

[그림 77] 문의하기에서 개인정보 노출 삭제 요청

3) 구글

구글(Google)의 저장된 페이지에서 개인정보가 노출될 경우, 구글에서 제공하고 있는 웹마스터 도구를 이용하여 검색엔진의 "저장된 페이지"(캐쉬)를 삭제요청 할 수 있습니다. 웹마스터 도구 삭제 요청 절차를 자세히 살펴보도록 하겠습니다.

[그림 78] 구글 검색엔진 2차 노출 조치 절차

구글 검색 결과에서 'URL 제거' 기능은 특정 사이트나 URL을 긴급 삭제하는 기능으로 웹사이트가 삭제되지 않더라도 구글 검색결과에서 임시 삭제됩니다. 임시적인 조치로 검색결과에서는 일정기간 동안만 보이지 않게 됩니다. 재노출될 가능성이 있으므로 웹사이트의 노출된 개인정보 삭제 후 'URL 제거' 기능을 이용해야 합니다.

① 구글 웹마스터 도구 로그인

[그림 79] 구글 웹마스터 도구 로그인

② 관리 사이트 추가

[그림 80] 속성추가 클릭

③ 작성

[그림 81] 사이트 URL 입력

④ 사이트 소유권 인증

[그림 82] HTML 파일 업로드

⑤ 사이트 추가 완료

[그림 83] 사이트 등록 화면

⑥ 개인정보 노출 사이트 선택

[그림 84] 삭제를 원하는 사이트 클릭

⑦ “URL 삭제” 메뉴선택

[그림 85] URL 삭제 클릭

⑧ 삭제 내용 작성

[그림 86] 일시적으로 숨기기 클릭

- 삭제할 URL 입력, 사이트 자체를 제거하려면 빈칸으로 두고 진행하면 됩니다.

[그림 87] 숨기기 목록에 추가됨

⑨ 삭제 사유 선택 및 신청완료

[그림 88] URL 삭제 목록에 추가

4) 빙(bing)

인터넷에 노출된 개인정보가 빙(bing) 검색엔진에 의한 2차 노출된 것을 발견하면, 아래와 같은 절차로 웹마스터도구에 방문하여 삭제 조치를 수행합니다.

[그림 89] 빙(bing) 검색엔진 2차 노출 조치 절차

① 빙 검색엔진의 웹마스터 도움말 페이지 접속

빙 검색엔진의 도움말 페이지의 “Bing에서 캐쉬된 페이지 제거” 버튼을 통해 캐쉬페이지 삭제 요청 페이지로 이동합니다.

[그림 90] 빙(bing) 웹마스터 도움말 페이지

② 콘텐츠 삭제 페이지에서 삭제할 URL 작성

빙 검색엔진의 웹마스터 〉 콘텐츠 삭제 페이지에서 삭제할 콘텐츠의 URL을 작성하여 삭제 요청합니다.

[그림 91] 빙(bing) 검색엔진 2차 노출 조치 절차

홈페이지 개인정보 노출방지 안내서

III

개인정보 노출, 예방할 수 있습니다!

- 홈페이지 운영자 개인정보 노출 예방수칙
- 홈페이지 개발자 개인정보 노출 예방수칙

III 개인정보 노출, 예방할 수 있습니다!

홈페이지 운영자 개인정보 노출 예방수칙

1. 게시판 운영 시 개인정보 노출 주의 안내하세요.

Key 게시글/댓글 작성 시 개인정보 노출 주의 안내

웹사이트 이용자 또는 관리자가 게시판 이용 시 개인정보 노출예방에 대한 안내를 받을 수 있도록 해당 페이지에 안내문구 및 팝업창 제공

제목	
작성자	◉ 전체공개 ○ 비공개
전화번호	
이메일	@ 직접 입력
내용	

등록 취소

2. 개인정보가 포함된 게시글 및 댓글 작성 시 비공개 설정하세요.

Key 게시글 및 댓글 비공개 설정

- 게시글에 대한 비공개 여부를 설정할 수 있는 기능 필요

- 개인정보가 포함되는 민원 페이지나 각종 신청 관련 게시판은 비공개 설정

3. 불가피하게 개인정보가 포함된 게시물 생성 및 게시글·댓글 작성 시에는 마스킹 등 비식별 처리하세요.

Key 불가피하게 개인정보가 포함된 게시물 및 게시글·댓글은 비식별 처리

- 이벤트 당첨, 합격자 공개 시 개인정보 마스킹

4. 첨부파일을 등록하기 전에 개인정보 유무 확인하세요.

Key 파일 업로드 전 개인정보 유무 확인 체크

- 첨부할 파일에서 불필요한 정보는 삭제 후 게시(업로드)
- 작성된 첨부 문서에서 개인정보의 포함여부 확인 후 게시(업로드)
  - [엑셀문서] 숨겨진 Sheet/행/열에 개인정보가 있는 지 확인
  - [엑셀문서] (메모)에 개인정보가 있는지 확인
  - [엑셀문서] OLE 객체(그래프 등)는 더블클릭 후 원본자료에 개인정보가 있는지 확인
  - [한글문서] 한글의 “개인정보 보호 기능”(보기메뉴)을 이용하여 개인정보 유무 확인
  - [이미지파일] 이미지 파일에 개인정보 포함 유무 확인
- 개인정보 검색 제품이 설치된 사용자 PC는 개인정보 사전검색 후 게시

5. 주기적으로 개인정보 노출 여부를 점검하세요.

Key 주기적인 개인정보 노출 점검

- 주기적인 점검 기본사항
  - 검색엔진(구글, 네이버, 다음 등) 확장기능을 이용한 개인정보 주기적 점검(검색단어 : “번호”, “주민”, “전화”, “여권” 등 활용)
- 웹사이트 변동(통합, 개선 등)시 점검사항
  - 개인을 구분하는 값으로 개인정보 사용여부 점검
  - 전송 및 저장시 개인정보 암호화 여부 점검
  - (개발 시) 시큐어 코딩을 적용하여 개발
  - (개발 후) 시큐어 코딩 준수여부 점검
  - 웹 취약점 점검

홈페이지 개발자 개인정보 노출 예방수칙

1. 관리자페이지를 안전하게 보호하세요.

Key 관리자페이지 접근제어 기능 적용

- 관리자페이지 접속은 SSL 기술을 이용하여 전송구간 암호화를 적용
- 관리자페이지는 접속이 필요한 관리자만 접근할 수 있도록 인가된 IP로 제한하는 기능 적용
- 관리자페이지는 가급적 내부망에서만 연결되도록 구성

관리자페이지 접근제한 설정

1. IIS 웹 서버(윈도우즈 서버)의 경우
   - "설정 > 제어판 > 관리도구 > 인터넷 서비스 관리자" 선택
   - 해당 관리자페이지 폴더에 오른쪽 클릭을 하고 등록정보 > 디렉터리 보안 > IP 주소 및 도메인 이름 제한 > 편집 버튼을 클릭
   - 액세스 거부를 선택하고 추가 버튼을 클릭하여 관리자 호스트IP 또는 서브넷을 등록

2. Tomcat 서버의 경우
   - $CATALINA_HOME(톰캣 홈 디렉터리)/conf/server.xml 파일 내용 중 〈Host〉 부분
   - 필드 사이에 아래와 같은 설정을 추가한 후 서버를 재시작하면 관리자페이지에 대해 IP기반으로 허용된 IP만 접근이 가능하도록 제어가 가능

〈관리자페이지 접근제한 설정〉

```
<Host ...>
<Context path="/KISAadm" docBase="/tomcat/webapps/ROOT/KISAadm">
<Valve className="org.apache.catalina.valves.RemoteHostValve"
       allow="192.168.1.2"/>
</Context>
</Host>
```

※ 한국인터넷진흥원 웹사이트(http://www.kisa.or.kr) > 자료실 > 관련법령·기술안내서 > 기술안내서 가이드 > 홈페이지 개발보안 안내서(p40), 홈페이지 취약점 진단제거 가이드(p67)

2. 게시판은 비공개 또는 비밀글 설정이 가능하도록 구축하세요.

Key 게시판을 비공개와 공개로 구분할 수 있도록 기능 적용

- 게시글에 개인정보 포함시 비공개 또는 비밀글로 설정할 수 있는 기능 적용
- 비밀글은 작성자만 열람할 수 있도록 적용

3. 접속경로(URL) 설정, 소스코드 개발 등에 개인정보를 사용하지 마세요.

Key 접속경로(URL)에 개인정보 삭제

- 회원정보 페이지 개발 시 접속경로(URL)에 생년월일, 주민등록번호 등 사용 금지

  ex) http://www.test.or.kr/board.php?search=info&list=

- 소스코드 내에 회원 식별자로 주민등록번호 등 사용 금지

4. 접속경로(URL) 식별자는 '숨김' 처리하여 보호하세요.

Key 홈페이지 설계시 POST 방식 이용

홈페이지 설계 시 페이지 구분 값 등으로 개인정보를 사용하는 경우 URL에 개인정보가 노출됩니다. 웹브라우저 주소 표시줄에 개인정보가 노출되지 않도록 GET 방식 보다는 POST 방식을 사용해야합니다.

- URL내 개인정보 등이 노출되지 않도록 POST 방식을 이용
  ex) http://www.test.or.kr/board.php

5. 홈페이지 개편 시 웹·소스코드 취약점 점검하세요.

Key 소스코드 등을 통한 개인정보 및 서버정보 등 노출 사전점검

- 소소코드 내 개인정보 포함여부 점검

```
29 /*본인요청으로 삭제(2017.11.09)*/
30 /*if(''=="topstand" && '' == "2") {alert("실명제 적용에 따라 '반[redacted]'님은 '오[redacted]'님으로
31 성명이 변경처리 되었습니다.\n\n이와 관련하여 문의사항은 전산과 [redacted]로 연락주시기 바랍니다.");}*/
```

웹페이지 소스코드 주석

- 소스코드 주석, 개발/테스트를 위한 에러 메시지 등에 서버정보 포함여부 확인

Forbidden

You don't have permission to access / on this server.

Apache/2.2.3 (CentOS) Server at [redacted] kr Port 80

에러 페이지 내 서버정보 포함

모든 웹 페이지에 대해 개발단계에서 디버깅 및 테스트를 목적으로 작성한 주석구문에 서버 주요 정보가 포함되어 있을 경우 공격자가 해당 정보를 다른 취약점과 연계해 사용할 수 있으므로 제거해야 합니다.

6. 디렉터리 리스팅 여부를 점검하세요.

Key 주기적인 디렉터리 리스팅 취약점 점검

- 주기적인 점검 기본사항
  - 검색엔진(구글, 네이버, 다음 등) 확장기능을 이용하여 내 홈페이지의 관리자페이지가 리스팅되고 있는지 주기적 점검
    (웹 서버의 URL로 "도메인네임 + 디렉터리" 경로를 입력하여 웹브라우저에 해당 디렉터리 등 모든 파일목록이 노출되는지 점검)

- 디렉터리 리스팅 노출 방지 설정
  - [Apache] indexes "문자열"제거
  - [Tomcat] Param-value 값을 "False" 로 설정
  - [Nginx] Autoindex 값을 "off"로 설정
  - [윈도우 인터넷 정보서비스(IIS)] 제어판 〉 관리도구 〉 인터넷서비스 관리자 〉 기본 웹사이트 속성 정보 수정(디렉터리 검색 부분을 비활성화)

FAQ

무엇이든 물어보세요

FAQ 무엇이든 물어보세요

Q 국세, 지방세 등을 체납하여 공시송달 시 납세의무자의 소재가 불분명하여 홈페이지를 통해 납세고지사항을 공시하고 있는데, 이 경우 납세자의 개인정보(이름, 주민등록번호, 주소 등)는 어느 범위까지 공개 가능한가요? 또한, 일부 체납자는 납세고지사항을 확인하지 못했다며 민원을 제기하는 경우도 있습니다. 세금 납부가 확인될 때까지 해당 내용을 계속 게시해도 되나요?

A 체납에 의한 공시송달 시 다음과 같이 관련법에 의거 납세자의 개인정보(이름, 주민등록번호, 주소 등)를 공개할 수 있습니다.

국세에 의한 공시송달의 경우 국세기본법 시행규칙 제5조 별지서식에 따라 성명, 주민등록번호, 사업자등록번호, 주소 또는 영업소, 상호, 서류의 명칭, 서류의 주요 내용을 기재해야 합니다. 또한 지방세에 의한 공시 송달의 경우 지방세기본법 시행규칙 별지 제10호 서식에 따라 송달 대상자의 성명 또는 법인명, 서류의 송달지, 서류의 명칭, 서류의 내용을 기재하도록 하고 있습니다.

공시송달은 행정절차법 제15조제3항에 의거 공고한 날로부터 14일이 지나면 송달이 된 것으로 간주되므로 계속하여 공고하는 것은 바람직하지 않다고 보아야 할 것입니다.

참고

행정절차법 제15조(송달의 효력 발생) ③ 제14조제4항의 경우에는 다른 법령등에 특별한 규정이 있는 경우를 제외하고는 공고일부터 14일이 지난 때에 그 효력이 발생한다. 다만, 긴급히 시행하여야 할 특별한 사유가 있어 효력 발생 시기를 달리 정하여 공고한 경우에는 그에 따른다.

Q 홈페이지를 통해 채용 합격자 발표 시 합격자의 개인정보는 어느 범위까지 공개 가능한가요?

A 원칙적으로 합격자 발표는 개별적으로 연락하는 것이 권장됩니다. 그럼에도 불구하고 홈페이지에서 합격자를 공개해야하는 경우 개인정보 보호법 제3조제7항에 의거 지원자 본인만 확인할 수 있도록 응시번호 또는 수험번호만 기재하거나 성명의 일부분을 홍*동 처럼 마스킹 처리하는 것이 바람직합니다. 다만, 동명이인의 구별 등을 위하여 성명 이외의 다른 정보(생년월일, 아이디, 연락처 등)를 함께 게시하는 경우에는, 성명의 일부 마스킹과 함께 생년월일이나 연락처 등도 일부를 마스킹 해야 합니다.

참고

개인정보 보호법 제3조(개인정보 보호 원칙) ⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

Q 공무원이나 공공기관 임직원 정보(이름, 전화번호 등)를 홈페이지를 통해 공개해도 되나요?

A 공무원이나 공공기관 임직원 정보는 정보공개법 제9조제1항제6호에 의거 홈페이지를 통해 공개해도 됩니다.

공무원 및 공공기관 임직원은 원활한 대민서비스 등 국민의 편의를 진작하고 친절한 서비스 제공 등의 업무진행을 위하여 [조직(부서명), 성명, 사무실 전화번호, 직급/직위, 담당업무] 정도를 기관이나 조직의 홈페이지에 공개하는 것이 일반적입니다.

이러한 점은 개인정보 보호법 제15조제1항제4호 및 제6호에 의거하여 적법한 개인정보의 수집 및 이용의 범위에 들어간다고 해석될 수 있습니다.

그러나 특정 공무원의 집주소, 개인휴대전화번호, 학력 및 경력 등은 공개하지 않는 것이 원칙이며, 랜섬웨어나 악성코드 삽입 이메일 급증 등 범죄에의 악용 우려를 고려해 볼 때 업무상 이메일주소는 공개하지 않는 것이 바람직할 것입니다.

참고

정보공개법 제9조(비공개 대상 정보) ① 공공기관이 보유·관리하는 정보는 공개 대상이 된다. 다만, 각 호의 어느 하나에 해당하는 정보는 공개하지 아니할 수 있다.

6. 해당 정보에 포함되어 있는 성명 주민등록번호 등 개인에 관한 사항으로서 공개될 경우 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되는 정보. 다만, 다음 각 목에 열거한 개인에 관한 정보는 제외한다.
   가. 법령에서 정하는 바에 따라 열람할 수 있는 정보
   나. 공공기관이 공표를 목적으로 작성하거나 취득한 정보로서 사생활의 비밀 또는 자유를 부당하게 침해하지 아니하는 정보
   다. 공공기관이 작성하거나 취득한 정보로서 공개하는 것이 공익이나 개인의 권리 구제를 위하여 필요하다고 인정되는 정보
   라. 직무를 수행한 공무원의 성명·직위
   마. 공개하는 것이 공익을 위하여 필요한 경우로서 법령에 따라 국가 또는 지방자치단체가 업무의 일부를 위탁 또는 위촉한 개인의 성명·직업

Q 홈페이지를 통해 청년구직수당 등 각종 수당 지급대상자를 발표·공개하려고 합니다.
수급자의 개인정보는 어느 범위까지 공개 가능한가요?

A 청년구직수당 등 각종 수당의 경우 중앙행정기관 및 지자체별로 자격 및 요건 등 상이한 기준으로 운용되고 있습니다. 관련 법령 및 자체의 조례 內 상기 내용을 포함하였다면 해당 규정에 따라 운용하면 됩니다. 하지만 관련 법령 및 조례가 없을 경우 개별적으로 연락하는 것이 권장됩니다. 부득이 홈페이지를 통해 공개해야할 경우 지원자 본인만 확인할 수 있도록 개인정보를 마스킹 처리하는 것이 바람직합니다.

Q 학원을 홍보하기 위해 홈페이지에서 학원생들의 각종 경진대회, 공모전, 콩쿠르 등의 입상 결과(이름, 사진, 학교, 학년 등)를 공개해도 되나요?
수급자의 개인정보는 어느 범위까지 공개 가능한가요?

A 학원이 당초 학원생들의 개인정보를 수집·이용하는 과정에서 입상결과 공개와 관련하여 사전 동의를 받았을 경우에만 공개할 수 있습니다. 이 때 학원생이 만14세 미만일 경우 개인정보 보호법 제22조(동의를 받는 방법)제6항에 따라 법정대리인의 동의(학생이 만 14세

미만일 경우)를 받아야 합니다.
만일 입상결과 공개와 관련하여 동의 받지 않고 후에 공개할 경우 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)에 따라 처벌 받게 됩니다.

Q 홈페이지 게시판에 이용자가 자신 또는 타인의 개인정보를 스스로 게재하는 경우에도 홈페이지 운영자가 관리해야 하나요?

A 정보통신망법 제32조의3(노출된 개인정보의 삭제·차단)에 의거 홈페이지 운영자는 상기와 같이 이용자 개인정보 게재 행위까지도 관리해야 합니다. 홈페이지관리자는 홈페이지 내 주의 문구를 삽입하여 이용자가 홈페이지에 개인정보를 게재하지 않도록 안내해야합니다.

※ 자세한 사항은 35페이지([그림 47] 게시글 작성 시 개인정보 노출에 대한 경고문구 삽입(예시)) 참고 바랍니다.

참고

정보통신망법 제32조의3(노출된 개인정보의 삭제 · 차단) ① 정보통신서비스 제공자등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다. ② 정보통신서비스 제공자등은 방송통신위원회 또는 한국인터넷진흥원의 요청이 있는 경우 제1항의 노출된 개인정보에 대한 삭제·차단 등 필요한 조치를 취하여야 한다.

Q 홈페이지 게시판에 일부 회원의 개인정보가 노출되어 있는 것을 확인하고 즉시 삭제 조치했는데도, 구글 등 검색사이트에서 해당 게시물이 계속 검색됩니다. 어떻게 해야 하나요?

A 노출된 개인정보를 해당 웹사이트에서 삭제하였더라도 구글 등 검색사이트에 기 노출된 정보가 저장되어 검색 시 2차 노출될 수 있습니다. 따라서 51페이지(나. 검색엔진별 개인정보 노출 조치 방안) 참고하셔서 검색사이트에 저장된 페이지를 삭제해야 합니다.

Q 구글 등 검색사이트에서 우리 기관 홈페이지의 관리자페이지가 검색·노출되고 있습니다. 관리자페이지가 검색되지 않도록 할 수 있는 방법이 있을까요?

A 관리자페이지가 구글 등 검색사이트를 통해 검색·노출되면 해커로부터 공격 받을 수 있으므로 http://OOO.co.kr/admin, /administrator 등 예측하기 쉬운 디폴트 주소를 사용해서는 안 됩니다. 만일 관리자페이지가 인터넷에 검색·공개되었다면 내부직원들만이 알 수 있는 주소로 변경하고, 외부에서 관리자페이지에 접속해야 한다면 안전한 접속수단 혹은 추가인증수단을 마련해야 합니다.

※ 자세한 사항은 15페이지([여기서, 잠깐!] 관리자페이지 안전하게 보호하기) 참고하시기 바랍니다.

Q 동호(창)회 회원들의 친목 도모를 목적으로 홈페이지를 통해 회원 연락처(이름, 휴대전화번호 등)를 게시 공유해도 되나요?

A 동호(창)회 회원들의 친목 도모를 위해 회원 간에 연락처를 공유하는 경우라면 개인정보보호법 제58조제3항에 의거 홈페이지에 공유해도 됩니다. 단, 관련법령은 제15조(개인정보의 수집·이용), 제30조(개인정보처리방침 수립·공개), 제31(개인정보책임자 지정)에 한해서만 제외되고 나머지 법조항은 모두 적용됩니다. 따라서 목적외 이용, 제3자 제공, 안전성확보조치 수립 등의 의무는 여전히 부과되므로 회원에 한해서만 열람 가능하도록 주의하고, 친목 도모 외의 목적으로 이용하거나, 회원이 아닌 제3자에게 정보를 제공해서는 안됩니다.

참고

개인정보 보호법 제58조(적용의 일부 제외) ③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.

Q 소규모 비영리 단체 홈페이지를 운영하고 있는데, 웹 취약점 점검을 반드시 받아야 하나요?

A 개인정보의 안전성 확보조치 기준 제6조제8항에 따르면 1만명 미만의 개인정보를 보유한 소규모 비영리 단체는 웹 취약점 점검 대상이 아닙니다. 반면, 1만명

이상의 개인정보를 보유한 소규모 비영리 단체는 웹 취약점 점검을 연 1회 이상 수행해야합니다.

KISA 인터넷보호나라&KrCERT(www.krcert.or.kr)에서 웹 취약점 점검을 무료로 서비스하고 있습니다. 해당 서비스는 '중소기업기본법 제2조'에 해당하는 중소기업까지 제공되므로, 소규모 비영리 단체도 이용할 수 있습니다.

참고

개인정보의 안전성 확보조치 기준 제6조(접근통제) ④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다. ⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

[그림 92] KISA 인터넷 보호나라 웹 취약점 점검 신청 페이지

홈페이지 개인정보 노출방지 안내서

부록

[부록 1] 주요 용어 이해하기
[부록 2] 개인정보 노출 점검, 스스로 해보기
[부록 3] 개인정보 유출 시 필수 조치사항
[부록 4] 주요 개인정보 8종 정규표현식
[부록 5] 참고자료

[부록 1] 주요 용어 이해하기

이 안내서에서 사용하는 용어의 뜻은 다음과 같습니다.

용어	용어 정의
개인정보	살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말합니다. (개인정보 보호법 제2조)
개인정보 마스킹	개인정보 보호를 위해 주민등록번호, 의료보험번호, 여권번호, 운전면허번호 같은 개인정보의 일부분을 인지할 수 없도록 비식별화하는 것입니다.
개인정보 검색 솔루션	웹사이트 내에 존재하는 개인정보를 검색하여 개인정보의 위치를 확인해주는 솔루션입니다.
개인정보 차단 솔루션	웹사이트에 자료를 올리거나, 게시판에 글 작성 시 컨텐츠에 개인정보 존재 유무를 확인해주는 솔루션입니다.
개인정보처리자	업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말합니다. (개인정보 보호법 제2조)
개인정보취급자	개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자를 뜻합니다. (개인정보 보호법 제28조)
검색엔진 (Search Engine)	검색엔진이란 인터넷 상에서 자료를 쉽게 찾을 수 있도록 검색사이트가 구축한 시스템입니다. 검색엔진은 정보수집·정보가공·정보제공의 세 가지 기능으로 구성되는데 정보수집은 크롤러, 정보가공은 인덱서, 정보제공은 사용자 인터페이스가 담당합니다. 크롤러가 인터넷을 검색하여 수집한 정보들을 인덱서를 이용하여 데이터베이스화 하고, 사용자가 검색어를 입력하면 사용자 인터페이스가 관련된 정보의 위치를 알려 줍니다.
공공기관	공공기관은 개인정보 보호법 제2조에 따르면 다음과 같습니다. 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체 (개인정보 보호법 제2조) 나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관

용어	용어 정의
디렉터리 (Directory)	디지털 자료 저장장치인 하드디스크에 저장된 파일들을 담고 있는 영역을 말하며, 디렉터리에는 그 속에 저장된 각각의 파일에 대한 이름과 크기, 위치 등이 기록되어 있습니다.
디렉터리 리스팅 취약점 (Directory Listing Vulnerability)	WEB이나 FTP 서비스의 취약한 설정으로 인해 서버의 디렉터리 및 파일에 열람 및 다운로드가 가능하게 되는 취약점입니다. 인터넷 사용자가 모든 디렉터리 및 파일 목록을 볼 수 있어 비공개 자료가 유출될 수 있습니다.
보이스피싱 (Voice Phishing)	전화를 통해 불법적으로 개인정보(주민등록번호, 신용카드번호, 은행계좌번호 등)를 빼내 범죄에 사용하는 신종 전화 사기 수법입니다. 음성(voice), 개인정보(personal information) 및 낚시(fishing)를 합성한 신조어입니다. 기존의 피싱은 이메일을 통해 중요 정보를 입력하게 하는 소극적인 방법인 데 반해, 보이스피싱은 범행 대상자에게 전화를 걸어 송금을 요구하거나 개인정보를 수집하는 적극적인 방법입니다.
소스코드 (Source Code)	컴퓨터 프로그램을 (사람이 읽을 수 있는) 프로그래밍 언어로 기술한 글을 말합니다.
스팸 (Spam)	수신자의 의사와 관계없이 인터넷상의 다수 수신인에게 전자 우편(e-mail), 문자메시지 등을 이용하여 무더기로 발송된 광고나 선전물을 의미합니다.
엑셀 (Excel)	미국 마이크로소프트(MS)사에 개발한 PC 용 수치관리 프로그램을 의미합니다. 많은 스프레드시트를 연결, 통합하여 다양한 도형과 차트 등 설명 자료를 작성하는 기능을 제공합니다.
웹 서버 (Web Server)	웹 페이지가 들어 있는 파일을 사용자들에게 제공하는 프로그램입니다. 웹 사이트를 통해 서비스를 하려면 웹 서버 프로그램을 설치해야 합니다. 보편적인 웹 서버로는 IIS와 아파치 등이 있습니다.
전용선	보안 등을 이유로 연결되는 노드간에 독점 사용하는 회선을 말합니다.
정규표현식	특정한 규칙을 가진 문자열의 집합을 표현하는 데 사용하는 형식 언어입니다. 정규표현식은 많은 텍스트 편집기와 프로그래밍 언어에서 문자열의 검색과 치환을 위해 사용하고 있습니다.
정보주체	처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말합니다. (개인정보 보호법 제2조)
개인정보의 처리	개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말합니다. (개인정보 보호법 제2조)
캐쉬 (Cache)	데이터 접근을 빠르게 할 수 있도록 미래의 요청에 대비해 데이터를 일시 저장해 두는 장소를 말합니다.
크롤러 (수집기)	검색엔진의 정보수집 부분을 담당하는 소프트웨어로 방대한 웹 페이지를 주기적으로 방문하여 각종 정보를 자동으로 수집합니다. 스파이더, 로봇, 봇, 웹수집기, 로봇 에이전트 등 다양한 이름으로 불리기도 합니다.
팝업창	특정 웹 사이트가 어떠한 내용을 표시하기 위해 추가로 생성되는 새 창을 말합니다.

용어	용어 정의
포워드 (Forward)	클라이언트가 접속한 서버에서 다른 서버로 페이지 변경이 발생하는 경우를 말합니다.
포털사이트 (Portal Site)	인터넷의 출발점과 관문이 되는 사이트를 말하는데, 초기에는 인터넷을 항해하기 위한 출발점으로서의 역할만을 수행하였습니다. 그러나 현재는 특정 주제를 가지고 한 영역에서 전문정보를 제공하는 서비스나 필요한 모든 서비스를 한 사이트를 통해 제공받는 서비스를 의미합니다.
휴면 웹사이트	휴면 웹사이트는 장기간 동안 접속자가 없거나 관리가 이루어지지 않고 방치된 웹 사이트를 말합니다.
OLE (Object Linking and Embedding)	응용프로그램 간 서로 호환이 되어 다른 응용 S/W에서 작성한 그림이나 표, 차트, 비디오 등과 같은 데이터의 정보를 연결시켜 주는 기능을 뜻합니다.
VPN (Virtual Private Network)	인터넷망을 전용선처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 기술로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용합니다.
URL (Uniform Resource Locator)	흔히 URL을 웹 사이트 주소로 알려져 있지만, 이는 웹 사이트 주소뿐만 아니라 컴퓨터 네트워크 상의 모든 자원을 나타낼 수 있습니다. URL은 주 컴퓨터의 이름과 주소, 파일이 있는 디렉터리 위치, 파일 이름으로 구성됩니다.
시큐어 코딩	개발하는 소프트웨어가 복잡해짐으로 인해 보안상 취약점이 발생할 수 있는 부분을 보완하여 프로그래밍 하는 것. 시큐어 코딩에는 안전한 소프트웨어를 개발하기 위해 지켜야 할 코딩 규칙과 소스 코드 취약 목록이 포함됩니다.
SSL (Secure Sockets Layer)	인터넷 프로토콜(Internet protocol)이 보안면에서 기밀성을 유지하지 못한다는 문제를 극복하기 위해 개발되었습니다. 현재 전세계에서 사용되는 인터넷 상거래시 요구되는 개인정보와 크레디트카드 정보의 보안 유지에 가장 많이 사용되고 있는 프로토콜이며, 최종 사용자와 가맹점간의 지불 정보 보안에 관한 프로토콜이라고 할 수 있습니다.

[부록 2] 개인정보 노출 점검, 스스로 해보기

기관·기업은 개인정보가 노출되고 있는지를 검색엔진을 통해 모니터링할 수 있습니다. 홈페이지관리자는 자신이 관리하는 사이트에서 검색엔진에 의한 개인정보 노출이 있는지 주기적으로 자가점검을 수행하고 검색엔진에 개인정보가 노출되었다면 즉시 조치를 취해야 합니다. 네이버, 구글 등 검색엔진의 기본검색이나 고급검색 기능을 활용하여 자체적으로 점검할 수 있습니다.

참고

주요 노출 키워드(예시)

번호	탐지어	번호	탐지어	번호	탐지어
1	주민등록번호	2	여권번호	3	운전자번호
4	외국인등록번호	5	이력서 filetype:doc	6	이력서 filetype:xls
7	여행 문의 + 여권번호	8	회원명단 filetype:xls	9	입사지원서 filetype:xls
10	주민등록번호 txt	11	학생명단 xlsx	12	교육생 명단 filetype:xls

1단계(구글(google.co.kr)에 접속)

[그림 93] 구글 검색 화면

2단계(기본검색/고급검색을 사용하여 개인정보 자가점검 수행)

1) 기본검색

구글 기본검색은 검색어를 입력하여 특정 검색어를 포함하거나, 특정 검색어를 제외하여 검색하는 등 기본적인 검색 기능을 제공합니다.

구분	연산자	검색예시
특정단어 포함	“”	구글 “입사지원서”
둘 다 포함	and, 공백	구글 입사지원서, 구글 and 입사지원서
둘 중에 하나 포함	OR(대문자), |	구글 OR 입사지원서
특정단어 제외	-	구글 - 입사지원서

2) 고급검색

고급검색은 검색 범위를 특정 사이트로 제한하거나, 특정 파일만 검색하는 등 특정 명령어를 이용하여 원하는 결과값을 쉽게 얻을 수 있는 기능입니다.

명령어	설명	검색예시
site	검색 범위를 특정 도메인으로 제한	site:kisa.or.kr 입사지원서
filetype	특정한 확장자를 가진 파일 검색	filetype:hwp 입사지원서
inurl	문자열을 페이지의 URL에서 검색	inurl:kisa.or.kr 입사지원서
intitle	페이지의 제목에서 문자열 검색	intitle:안녕 입사지원서
- (마이너스)	원하지 않는 단어를 제외하고 검색	입사지원서 신청서

기본검색 또는 고급검색을 이용하여 아래와 같이 개인정보의 유출이 있는지 점검합니다.

[그림 94] 구글 고급검색 예시

[부록 3] 개인정보 유출 시 필수 조치사항

온·오프라인을 통해 고객(이용자)의 개인정보를 수집·이용하는 기관이나 기업은 해킹 등으로 개인정보 유출이 발생한 경우 개인정보 보호 관련 법령에 따라 해당 정보주체(이용자)에게 지체 없이 통지하여야 합니다. 또한, 개인정보 유출로 인한 피해를 최소화하기 위해 필요한 긴급 조치를 이행하고, 그 조치 결과를 관계 중앙행정기관(행정안전부, 방송통신위원회) 또는 한국인터넷진흥원에 지체 없이 신고하여야 합니다.

[그림 95] 개인정보 유출 시 필수 조치요령

「개인정보 보호법」을 적용받는 정부 공공기관 및 비영리 협·단체 등의 경우, 정보주체에 대한 개인정보 유출 통지는 유출되었음을 알게 된 후 5일 이내 통지해야 하며, 유출 신고는 1천명 이상 정보주체의 개인정보 유출 시에 행정안전부(www.privacy.go.kr) 또는 한국인터넷진흥원에 신고하도록 하고 있습니다.

보다 자세한 사항은 개인정보보호 종합포털(www.privacy.go.kr) - 자료마당 참고자료 매뉴얼의 '표준 개인정보 유출사고 대응 매뉴얼'을 참고하시기 바랍니다.

참고

「개인정보 보호법」 상의 개인정보 유출 통지 신고 근거 법령

제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정안전부장관 또는 대통령령으로 정하는 전문기관은 피해 확산 방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

〈 개인정보 보호법 시행령 〉

제40조(개인정보 유출 통지의 방법 및 절차) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 서면등의 방법으로 지체 없이 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검 보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있다.

② 제1항에도 불구하고 개인정보처리자는 같은 항 본문에 따라 개인정보가 유출되었음을 알게 되었을 때나 같은 항 단서에 따라 유출 사실을 알고 긴급한 조치를 한 후에도 법 제34조제1항제1호 및 제2호의 구체적인 유출 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면 등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

③ 제1항과 제2항에도 불구하고 법 제34조제3항 및 이 영 제39조제1항에 따라 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 법 제34조제1항 각 호의 사항을 7일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 서면등의 방법과 함께 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 7일 이상 게시하여야 한다.

개인정보보호 종합포털(www.privacy.go.kr)을 통한 개인정보 유출 신고 절차는 다음과 같습니다.

① 개인정보보호 종합포털 (www.privacy.go.kr) 접속

② 자주찾는 서비스 내 '개인정보 유출신고' 클릭(또는 민원마당 - '개인정보 유출신고' 클릭)

③ 개인정보 유출신고 안내 사항 확인

④ '개인정보 유출신고' 클릭

⑤ 개인정보 유출신고서 작성 및 제출

HOME > 민원마당 > 개인정보 유출신고

민원마당

- 개인정보 열람등요구
- 개인정보 침해신고
- 본인확인내역 통합조회
- 개인정보 유출신고
- 개인정보 분쟁조정

개인정보 유출신고

인쇄하기 + -

개인정보 유출신고 안내 | 개인정보 유출신고

유출신고

개인정보처리자는 정보주체의 개인정보가 유출된 경우(1천명 이상인 경우에는 필수의무사항-개인정보보호법 제34조 동법 시행령 제39조)에 정보주체에 대한 통지 및 조치 결과를 지체없이 신고하여야 합니다.
개인정보에 대한 침해를 신고하시려면 '개인정보 침해신고'를 이용해주시고, 개인정보 유출신고는 반드시 개인정보처리자만 신고해주시기 바랍니다.

"*" 는 필수 입력정보 입니다.

신고기관 *					
신고기관 유형 *	◉ 기관 ○ 일반사업자 ○ 기타				
정보주체 통지여부*	◉ 통지 ○ 미통지				
신고인 *	성명				
	연락처	- -			
	이메일				
유출된 개인정보의 항목 및 규모 *	0 / 4000 byte				
유출된 시점과 그 경위 *	0 / 4000 byte				
유출피해 최소화 대책, 조치 및 결과	0 / 4000 byte				
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	0 / 4000 byte				
	성명	부서	직위	연락처	이메일
개인정보보호 책임자 *					
개인정보취급자 *					

유출신고접수기관은 **행정안전부 및 유출신고 전문기관 담당자만 입력**하시면 됩니다.
유출신고를 하시는 개인정보처리자는 입력하실 필요가 없습니다.

신고하기

⑥ 개인정보 유출신고서 작성 예시

유출된 개인정보의 항목 및 규모 *	이름, 주소, 휴대전화 번호, 이메일, 주소 등 16만5000건의 개인정보 64 / 4000 byte
유출된 시점과 그 경위 *	내부직원이 어제 저녁 악성코드가 첨부된 이메일을 열람하고 악성코드에 감염되었고 (5.3 오후 16:38), 이메일을 열람한 내부직원의 PC를 경유하여 파일공유서버에 악성코드가 설치되면서(5.3 오후17:41), 파일공유서버에 연결 된 개인정보 취급자 PC의 262 / 4000 byte
유출피해 최소화 대책, 조치 및 결과	각 이용자들이 개인정보 유출여부를 확인할 수 있도록 조회사이트를 개설하였으며, 홈페이지 개인정보 유출 통지문을 통해 이용자들께 공지를 한 상태입니다. 또한 탈취한 개인정보를 이용한 보이스피싱/운영자사칭/이메일을 통한 악성코드 유포 253 / 4000 byte
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	1. 지능형 스팸차단서비스를 이용한 스팸 차단 2. 수신 스팸메일 적극 신고 3. 비밀번호 변경 등 90 / 4000 byte

한편, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 적용받는 정보통신서비스 제공자 등은 1명 이상 이용자의 개인정보 유출이 발생한 경우, 유출되었음을 알게 된 후 24시간 이내 해당 이용자에게 개인정보 유출 통지를 해야 하며, 소관부처인 방송통신위원회 또는 한국인터넷진흥원(www.i-privacy.kr)에 유출 신고를 해야 합니다.

보다 자세한 사항은 온라인 개인정보보호 포털(www.i-privacy.kr) - 자료실 법규 및 지침 가이드라인의 '개인정보 유출 대응 매뉴얼'을 참고하시기 바랍니다.

참고

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 상의 개인정보 유출 통지·신고 근거 법령

〈 정보통신망 이용촉진 및 정보보호 등에 관한 법률 〉

제27조의3(개인정보 유출등의 통지·신고) ① 정보통신서비스 제공자 등은 개인정보의 분실·도난·유출(이하 "유출 등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다

1. 유출등이 된 개인정보 항목
2. 유출등이 발생한 시점
3. 이용자가 취할 수 있는 조치
4. 정보통신서비스 제공자등의 대응 조치
5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

② 제1항의 신고를 받은 한국인터넷진흥원은 지체 없이 그 사실을 방송통신위원회에 알려야 한다.

③ 정보통신서비스 제공자등은 제1항 본문 및 단서에 따른 정당한 사유를 방송통신위원회에 소명하여야 한다.

④ 제1항에 따른 통지 및 신고의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

⑤ 정보통신서비스 제공자등은 개인정보의 유출등에 대한 대책을 마련하고 그 피해를 최소화할 수 있는 조치를 강구하여야 한다.

〈 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 〉

제14조제2(개인정보 유출 등의 통지·신고) ① 정보통신서비스 제공자 등은 개인정보의 분실·도난·누출(이하 "유출등"이라 한다)의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.

② 정보통신서비스 제공자등은 제1항에 따른 통지·신고를 하려는 경우 법 제27조의3제1항 제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 아니하였으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.

③ 정보통신서비스 제공자등은 법 제27조의3제1항 각 호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제27조의3제1항 각 호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다.

④ 천재지변이나 그 밖의 정당한 사유로 제3항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고하는 것으로 제3항에 따른 홈페이지 게시를 갈음할 수 있다.

⑤ 정보통신서비스 제공자등은 법 제27조의3제1항 각 호 외의 부분 본문 및 단서에 따른 정당한 사유를 지체 없이 서면(전자문서를 포함한다)으로 방송통신위원회에 소명하여야 한다.

온라인 개인정보보호 포털(www.i-privacy.kr)을 통한 개인정보 유출 신고 절차는 다음과 같습니다.

① 온라인 개인정보보호 포털 (www.i-privacy.kr) 접속

② '개인정보 신고' 내 MORE 클릭 (또는 '개인정보 유출신고' - '개인정보 유출신고 하기' 클릭)

부록

③ 개인정보 유출신고 안내 사항 확인

④ '개인정보 유출신고하기' 클릭

⑤ 개인정보 유출신고서 작성 및 제출

개인정보신고

- 개인정보 유출신고
- 개인정보 유출신고 안내
- 개인정보 유출신고하기
- 주민번호 불법수집신고
- 개인정보 침해신고
- 개인정보 분쟁조정

개인정보 유출신고

개인정보 유출신고 작성 안내

- 개인정보 유출신고는 정보통신 서비스를 제공하는 사업자들을 대상으로 하는 신고제도입니다.
- 정보통신서비스 제공자등은 개인정보의 분실·도난·유출 사실을 안 때에는 지체 없이 방송통신위원회 신고와는 별도로 이용자에게도 통지하여야 합니다.
  ※ 관련근거 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제27조의3 제1항

※ 이용자의 개인정보 침해에 대한 신고는 '개인정보침해신고센터(e-클센터 118)를 이용부탁드립니다.

개인정보 유출신고 정보 입력

신고접수는 가급적 개인정보 취급자가 해주시기를 바랍니다.

* 필수 입력 항목입니다.

기관명*		사업자번호*	- -
사업자주소 (사업자등록기준)		웹사이트 주소	
유출된 개인정보의 항목 및 규모*	0 / 4000bytes		
유출이 발생된 시점, 유출 인지 시점 및 경위*	0 / 4000bytes		
이용자가 취할 수 있는 조치*	0 / 4000bytes		
정보통신서비스 제공자등의 대응조치*	0 / 4000bytes		

	성명	연락처(HP)	이메일
이용자 상담 담당부서 담당자 및 연락처*	개인정보 보호책임자	010 - -	
	개인정보 취급자	010 - -	

신고하기

부록

⑥ 개인정보 유출신고서 작성 예시

유출된 개인정보의 항목 및 규모*	이름, 주소, 휴대전화번호, 이메일주소 등 16만 5000건의 개인정보 39 / 4000bytes
유출이 발생된 시점, 유출 인지 시점 및 경위*	내부직원이 어제 저녁 악성코드가 첨부된 이메일을 열람하고 악성코드에 감염되었고(5.3 오후 16:38) 이메일을 열람한 내부직원의 PC를 경유하여 파일공유서버에 악성코드가 설치되면서(5.3 오후 17:41) 파일공유서버에 연결 된 개인정보 취급자의 PC의 개인정보를 탈취(5.4 오전 11:39) 유출이 되었습니다. 176 / 4000bytes
이용자가 취할 수 있는 조치*	1. 지능형 스팸자단서비스를 이용한 스팸자단 2. 수신 스팸메일 적극 신고 3. 비밀번호 변경 등 54 / 4000bytes
정보통신서비스 제공자등의 대응조치*	각 이용자들이 개인정보 유출여부를 확인할 수 있도록 조회사이트를 개설하였으며, 홈페이지 개인정보 유출통지문을 통해 이용자들께 공지를 한 상태입니다. 또한 탈취한 개인정보를 이용한 보이스피싱/운영자 사칭/이메일을 통한 악성코드 유포 등으로 발생할 수 있는 2차 피해를 자단하기 위해 개인정보 유출 의심계정에 대한 계정정지 조치를 하였습니다. 189 / 4000bytes

[부록 4] 주요 개인정보 8종 정규표현식

인터넷 상 개인정보 노출 모니터링을 위한 주요 개인정보 8종의 정규표현식은 다음과 같습니다.

주요 개인정보 8종 정규표현식

- 주민등록번호

```
(?<=[^0-9a-zA-Z])([0-9][0-9][01][0-9][0-3][0-9][\s-:\.]?)([1-4]\d{6})(?=[^0-9a-zA-Z])
```

- 여권번호

```
(?<=[^0-9a-zA-Z])([M|S|R|O|D|m|s|r|o|d][0-9]{8})(?=[^0-9a-zA-Z])
(?<=[^0-9a-zA-Z])([a-zA-Z]{2}[0-9]{7})(?=[^0-9a-zA-Z])
```

- 운전면허번호

```
(?<=[^0-9a-zA-Z])(\d{2}[\s-:\.])(\d{6}[\s-:\.])(\d{2})(?=[^0-9a-zA-Z])
```

- 핸드폰번호

```
(?<=[^0-9a-zA-Z])(01[0|1|6|7|8|9][\s-:\.]?)(\d{3,4}[\s-:\.]?)(\d{4})(?=[^0-9a-zA-Z])
```

- 신용카드번호

```
(?<=[^0-9a-zA-Z])(\d{4}[\s-:\.])(\d{4}[\s-:\.])(\d{4}[\s-:\.])(\d{4})(?=[^0-9a-zA-Z])
```

- 건강보험번호

```
(?<=[^0-9a-zA-Z])([1-9]\d{10})(?=[^0-9a-zA-Z])
```

- 계좌번호

```
(?<=[^0-9a-zA-Z])(\d{3}[\s-:\.])(\d{3}[\s-:\.])(\d{6})(?=[^0-9a-zA-Z])
(?<=[^0-9a-zA-Z])(\d{4}[\s-:\.])(\d{3}[\s-:\.])(\d{6})(?=[^0-9a-zA-Z])
(?<=[^0-9a-zA-Z])(\d{6}[\s-:\.])(\d{2}[\s-:\.])(\d{6})(?=[^0-9a-zA-Z])
(?<=[^0-9a-zA-Z])(\d{6}[\s-:\.])(\d{2}[\s-:\.])(\d{6})(?=[^0-9a-zA-Z])
(?<=[^0-9a-zA-Z])(\d{3}[\s-:\.])(\d{2}[\s-:\.])(\d{5}[\s-:\.])(\d{1})(?=[^0-9a-zA-Z])
(?<=[^0-9a-zA-Z])(\d{3}[\s-:\.])(\d{6}[\s-:\.])(\d{5})(?=[^0-9a-zA-Z])
(?<=[^0-9a-zA-Z])(\d{3}[\s-:\.])(\d{6}[\s-:\.])(\d{2}[\s-:\.])(\d{3})(?=[^0-9a-zA-Z])
```

- 외국인 등록번호

```
(?<=[^0-9a-zA-Z])([0-9][0-9][01][0-9][0-3][0-9][\s-:\.]?)([5-8]\d{6})(?=[^0-9a-zA-Z])
```

[부록 5] 참고자료

보다 안전한 홈페이지 구축 운영을 위해 홈페이지 설계 개발 단계부터 운영에 이르기까지 각 단계별로 도움을 받을 수 있는 유용한 공개 참고자료입니다.

NO	자료명	출처	다운로드 위치
1	표준 개인정보 유출사고 대응 매뉴얼 (2017.12)	행정안전부, 한국인터넷진흥원	개인정보보호 종합포털(privacy.go.kr) 〉 자료마당 〉 참고자료 〉 메뉴얼
2	[정보통신서비스 제공자등을 위한] 개인정보 유출 대응 매뉴얼 (2016.08)	방송통신위원회, 한국인터넷진흥원	온라인 개인정보보호 포털(i-privacy.kr) 〉 자료실 〉 법규 및 지침 게시판 〉 가이드
3	개인정보 비식별 조치 가이드라인 (2016.06)	방송통신위원회, 한국인터넷진흥원	온라인 개인정보보호 포털(i-privacy.kr) 〉 자료실 〉 법규 및 지침 게시판 〉 가이드
4	패스워드 선택 및 이용 안내서 (2016.02)	방송통신위원회, 한국인터넷진흥원	한국인터넷진흥원(kisa.or.kr) 〉 자료실 〉 기술안내서가이드
5	중소IT서비스 기업을 위한 정보보호 안내서 I (2016.02)	한국인터넷진흥원	한국인터넷진흥원(kisa.or.kr) 〉 자료실 〉 기술안내서가이드
6	중소IT서비스 기업을 위한 정보보호 안내서 II (2016.02)	한국인터넷진흥원	한국인터넷진흥원(kisa.or.kr) 〉 자료실 〉 기술안내서가이드
7	중소IT서비스 기업을 위한 정보보호 안내서 III (2016.02)	한국인터넷진흥원	한국인터넷진흥원(kisa.or.kr) 〉 자료실 〉 기술안내서가이드
8	주민등록번호 수집 금지 제도 가이드라인 (2014.01)	행정안전부	개인정보보호 종합포털(privacy.go.kr) 〉 자료마당 〉 지침자료

홈페이지 개인정보 노출방지
안내서

행정안전부
Ministry of the Interior and Safety

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY