개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-009호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	담양군청 전남 담양군 담양읍 추성로 1371
의결연월일	2021. 1. 27.

주 문

1. 피심인 담양군청에 대해 다음과 같이 시정조치를 권고한다.

가. 주민등록번호를 처리하는 경우에는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

나. 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

다. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급시 개인정보 취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

라. 가·나·다의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은「개인정보 보호법」제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로「지방자치법」제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[1]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 5. 19.~5. 22.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 주민등록번호를 안전하게 보관하지 않은 행위

피심인은 에서 주민등록번호를 평문으로 저장하고 있었다.

나. 개인정보 처리업무 위탁 시 수탁자 관리·감독을 소홀히 한 행위

피심인은 업무 위탁 관련 수탁자가 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리현황 점검 등 수탁자가 개인정보를 안전하게 관리하는지를 감독하지 않았다.

다. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 과 에서 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실이 있다.

- 에서 총괄관리계정을 각 부서담당이 공용사용함

2) 피심인은 에서 개인정보처리시스템의 접근 권한 변경·말소에 대한 내역을 기록하지 않은 사실이 있다.

---

1) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

3) 피심인은 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유한 사실이 있다.

4) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실이 있다.

- 수행업무 누락 :
- 처리한 정보주체의 정보 누락 :

5) 피심인은 에서 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제24조의2제2항은 "개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다"고 규정하고 있다.

나. 「개인정보 보호법」 제26조제4항은 "위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다"고 규정하고 있다.

1) ‘개인정보보호 법령 및 지침·고시 해설’(행정안전부, 2016.12)에 따르면 위탁자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. 또한, 위탁자는 수탁자가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위수탁 계약(법 제26조제1항 각호에 따른 사항)의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다. 따라서 위탁자는 수탁자에 대해 정기적인 교육을 실시하는 외에 수탁자의 개인정보 처리현황 및 실태, 목적외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.

다. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근권한의 제한 조치(제2호)’, ‘개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다.(제5조제2항)

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다.(제5조제3항)

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다(제5조제4항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다.(제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응

조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 주민등록번호를 안전하게 보관하지 않은 행위(법 제24조의2 제2항)

피심인은 에서 주민등록번호를 저장하는 경우 안전한 암호화 알고리듬을 이용하여 암호화 저장하여야 하나, 평문으로 저장한 행위는 「개인정보 보호법」 제24조의2 제2항을 위반한 것이다.

나. 개인정보 처리업무 위탁 시 수탁자 관리·감독을 소홀히 한 행위(법 제26조 제4항)

피심인은 업무 위탁 시 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자에 대한 교육 및 감독을 하지 않은 것은 「개인정보 보호법」 제26조제4항을 위반한 것이다.

다. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①가에서 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②
에서 개인정보처리시스템의 접근권한 변경·말소에 대한 내역을 기록하지 않은

사실(고시 제5조제3항), ③개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 사용자계정을 발급하지 않고 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ④개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑤에서 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(담양군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
주민등록번호 암호화 보관	§24의2②	-	주민등록번호 DB보관 시 암호화 등 안전한 보관 위반
수탁자 관리·감독	§26④	§28⑥	개인정보 처리 업무 위탁 시 수탁자의 개인정보 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지 관리· 감독하지 않음
안전조치의무	§29	§30	① 개인정보취급자가 변경되었을 경우, 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록하지 않음 (고시 제5조제3항) ③ 개인정보취급자별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유하여 사용함(고시 제5조제4항) ④ 접속자, 수행업무, 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리함(고시 제8조제1항) ⑤ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 주민등록번호를 처리하는 경우에는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

나. 피심인은 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·

변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

다. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급시 개인정보 취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

라. 가·나·다의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제24조의2제2항, 제26조제4항 및 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-010호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 영암군청
전남 영암군 영암읍 군청로1 영암군청

의결연월일 2021. 1. 27.

주 문

1. 피심인 영암군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

5) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

6) 암호화된 개인정보를 안전하게 보관하기 위해 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립할 것

7) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목 누락 없이 보관·관리할 것

8) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[2]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 5. 18.~5. 21.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 에서 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실이 있다.

2) 피심인은 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실이 있다.

3) 피심인은 개인정보취급자별로 사용자계정을 발급하지 않아 사용자계정이 다른 개인정보취급자와 공유된 사실이 있다.

4) 피심인은 에서 안전한 비밀번호 작성규칙을 수립하였으나, 이를 적용하지 않은 사실이 있다.

5) 피심인은 비밀번호를 저장하는 경우 일방향 암호화 적용을 하지 않은 사실이 있다.

6) 피심인은 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립하지 않은 사실이 있다.

7) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 보관·관리

2) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

하지 않은 사실이 있다.

8) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생

하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)
- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷홈페이지 등에 적용하여야 한다. 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 하며, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다. (제5조제5항)
- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된

사용자임을 확인한다. (제7조제2항)

- 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키, 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다. 암호 키는 암호화된 데이터를 복호화 할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며 라이프사이클 단계별 암호 키 관리 절차를 수립·시행하여야 한다. (제7조제6항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속 시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인

정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실(고시 제5조제3항), ③개인정보취급자 별로 사용자계정을 발급하지 않아 사용자계정을 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ④안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실(고시 제5조제5항), ⑤비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않은 사실(고시 제7조제2항), ⑥ 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립하지 않은 사실(고시 제7조제6항), ⑦개인정보취급자가 개인정보처리시스템에 접속한 기록을 보관·관리하지 않은 사실(고시 제8조제1항), ⑧개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(영암군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30	① 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않음 (고시 제5조제3항) ③ 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유됨 (고시 제5조제4항) ④ 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않음 (고시 제5조제5항) ⑤ 비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않음 (고시 제7조제2항) ⑥ 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립하지 않음 (고시 제7조제6항) ⑦ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 보관·관리하지 않음 (고시 제8조제1항) ⑧ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

5) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

6) 암호화된 개인정보를 안전하게 보관하기 위해 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립할 것

7) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

8) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하

여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-011호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	경상북도청 경상북도 안동시 풍천면 도청대로 455
의결연월일	2021. 1. 27.

주 문

1. 피심인 경상북도청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

2) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

3) 비밀번호를 정보통신망을 통하여 송신하거나 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[3]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 5. 18.~5. 21.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보취급자에 대한 감독을 소홀히 한 행위

1) 피심인은 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 하나, '18년 이후 개인정보취급자에게 필요한 교육을 실시하지 않은 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 에서 개인정보취급자별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유된 사실이 있다.

2) 피심인이 외부에서 에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실이 있다.

3) 피심인은 에서 개인정보취급자의 비밀번호를 정보통신망을 통하여 송신 시 암호화하지 않은 사실이 있다.

4) 피심인은 개인정보취급자가 에 접속한 기록 중 정보주체의 정보를 보관·관리하지 않은 사실이 있다.

---

3) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

5) 피심인은 에서 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제28조제2항은 “개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.”고 규정하고 있다.

1) ‘개인정보보호 법령 및 지침·고시 해설’(행정안전부, 2016.12)에 따르면 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다. 교육은 사내교육, 외부교육, 위탁교육 등 여러 종류가 있을 수 있으나 연간 교육계획을 수립하여 모든 개인정보취급자가 일정 시간 이상 교육에 참여하도록 해야 한다. 또한 개인정보취급자의 지위·직책, 담당업무의 내용, 업무 숙련도 등에 따라 교육 내용도 각기 달라져야 한다.

나. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용해야 한다. 인터넷 구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (제6조제2항)

- 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나, 보조저장매체를 통하여 전달하는 경우에는 이를 암호화

하여야 한다. 고유식별정보는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다. 비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다. 정보통신망이란 전기통시사업법 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다. (제7조제1항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)
- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고

적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보취급자에 대한 감독을 소홀히 한 행위 (법 제28조제2항)

피심인이 개인정보가 적정하게 취급되도록 개인정보취급자에게 교육을 실시하여야 하나, ’18년 이후 개인정보취급자에게 필요한 교육을 실시하지 않은 사실은 「개인정보 보호법」 제28조제2항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실(고시 제5조제4항, ②외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증 수단을 적용하지 않은 사실(고시 제6조제2항), ③개인정보취급자의 비밀번호를 정보통신망을 통하여 송신 시 암호화하지 않은 사실(고시 제7조제1항), ④접속기록 항목이 일부 누락된 개인정보취급자의 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑤개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(경상북도청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보 취급자 감독	§28②		개인정보취급자에게 정기적으로 필요한 교육을 실시하지 않음
안전조치의무	§29	§30	① 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유됨 (고시 제5조제4항) ② 외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증 수단을 적용하지 않았음 (고시 제6조제2항) ③ 개인정보취급자의 비밀번호를 정보통신망을 통하여 송신 시 암호화하지 않음 (고시 제7조제1항) ④ 접속기록 항목이 일부 누락된 개인정보취급자의 접속기록을 보관·관리함 (고시 제8조제1항) ⑤ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않았음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

2) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등

안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

3) 비밀번호를 정보통신망을 통하여 송신하거나 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제28조제2항, 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라, 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 홍 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-012호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 영천시청
경상북도 영천시 시청로 16

의결연월일 2021. 1. 27.

주 문

1. 피심인 영천시청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리할 것

2) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

3) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

4) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[4]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 5. 18.~5. 21.) 결과, 다음과 같은 사실을 확인하였다.

4) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보보호 책임자가 연 1회 이상 내부관리계획의 이행실태를 점검·관리하지 않은 사실이 있다.

2) 피심인은 접근권한 부여·변경·말소에 대한 내역을 기록·보관하지 않은 사실이 있다

3) 피심인은 전보 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실이 있다.

4) 피심인은 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실이 있다.

5) 피심인은 개인정보취급자가 접속한 기록 중 수행업무, 처리한 정보주체 정보 등을 누락하여 보관 관리한 사실이 있다.

6) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보의 안전한 처리를 위한 내부관리계획의 수립·시행(제1호)’, ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보 보호책임자는 내부관리계획의 적정성과 실효성을 보장하기 위하여 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행 실태를 연1회 이상으로 점검·관리하여야 한다. 내부관리계획의 이행 실태 점검·관리 결과에 따라 적절한 조치를 취하여야 하며, 중대한 영향을 초래

하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다. (제4조제4항)

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)
- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(인증서, OTP 등)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치를 취하여야 한다. (제5조제6항)
- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을

고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보 보호책임자를 통해 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않은 사실(고시 제4조제4항), ②전보 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ③개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ④계정정보 또는

비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실(고시 제5조제6항), ⑤개인정보처리시스템에 접속한 기록을 보관·관리하지 않거나 필수항목 중 일부가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑥개인정보처리시스템의 접속기록을 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(영천시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30	① 개인정보 보호책임자가 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않음 (고시 제4조제4항) ② 전보 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ③ 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ④ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않음 (고시 제5조제6항) ⑤ 개인정보처리시스템에 접속한 기록을 보관·관리하지 않거나, 필수항목 중 일부가 누락된 개인정보취급자의 접속기록을 보관·관리함 (고시 제8조제1항) ⑥ 개인정보처리시스템의 접속기록을 점검하지 않음(고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리할 것

2) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

3) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

4) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-013호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 청도군청
경상북도 청도군 화양읍 청화로 70

의결연월일 2021. 1. 27.

주 문

1. 피심인 청도군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보처리자는 개인정보 수집·이용 동의를 받을 때, 필수 고지 사항(수집 항목, 수집·이용목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 피심인은 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[5]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 5. 25.~5. 28.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 시 동의 받아야 할 사항을 고지하지 않은 행위

1) 피심인은 개인정보 수집·이용 동의 서식에 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에 그 불이익 내용을 고지하지 않고 개인정보를 수집한 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 전보 또는 퇴직 등 인사이동으로 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소하지 않은 사실이 있다.

2) 피심인은 접근권한 등록, 변경, 말소에 대한 내역을 기록·보관하지 않은 사실이 있다.

3) 피심인은 개인정보취급자별로 사용자계정을 발급하지 않아 사용자계정이 다른 개인정보취급자와 공유된 사실이 있다.

4) 피심인은 개인정보취급자의 접속기록을 일부 누락하여 보관·관리한 사실이 있

5) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

다.

5) 피심인은 접속기록을 월1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제15조제2항은 “개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다”고 규정하고 있으며, 이 때 알려야 할 사항은 ①개인정보의 수집·이용목적, ②수집하려는 개인정보의 항목, ③개인정보의 보유 및 이용기간, ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용이다.

나.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보의 안전한 처리를 위한 내부관리계획의 수립·시행(제1호)’, ‘개인정보침해사고 발생에 대응하기 위한

접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)
- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보 수집 시 고지를 소홀히 한 행위 (법 제15조제2항)

피심인이 개인정보 수집·이용 동의를 받을 때, 필수 고지사항(“동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용”)을 알리지 않고 개인정보를 수집한 사실은 「개인정보 보호법」 제15조제2항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ③개인정보취급자 별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유하여 사용한 사실(고시 제5조제4항), ④접속자, 수행업무, 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑤개인정보처리시스템의 접속기록을 1월 이상 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(청도군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보 수집·이용 동의	§15②	-	개인정보 수집·이용 동의를 받을 때 필수 고지사항(”동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용”)을 알리지 않음
안전조치의무	§29	§30①	① 개인정보취급자가 변경되었을 경우, 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ③ 개인정보취급자별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유하여 사용함 (고시 제5조제4항) ④ 접속자, 수행업무, 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리함 (고시 제8조제1항) ⑤ 개인정보처리시스템의 접속기록을 1월 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보 수집·이용 동의를 받을 때, 필수 고지사항(수집항목, 수집·이용목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 피심인은 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제15조제2항 및 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등)제4항에 따라, 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-014호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	양양군청 강원도 양양군 양양읍 군청길 1
의결연월일	2021. 1. 27.

주 문

1. 피심인 양양군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여할 것

2) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[6]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 5. 25.~5. 28.) 결과, 다음과 같은 사실을 확인하였다.

---

6) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하고 있지 않은 사실이 있다.

2) 피심인은 전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실이 있다.

3) 피심인은 개인정보취급자별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유한 사실이 있다.

4) 피심인은 개인정보취급자의 비밀번호를 일방향 암호화 저장하지 않은 사실이 있다.

5) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목*이 누락된 접속기록을 보관·관리한 사실이 있다.

* 수행업무 누락

6) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2021. 1.22. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 개인정보처리시스템에 대한 접근권한을 업무 수행목적에 따라 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 접근통제를 위한 안전조치를 취해야 한다. 특히, 개인정보처리시스템의 데이터베이스(DB)에

대한 직접적인 접근은 데이터베이스 운영·관리자에 한정하는 등의 안전조치를 적용할 필요성이 있다. (제5조제1항)

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다. (제7조제2항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년

이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하지 않은 사실(고시 제5조제1항), ②전보

또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ③개인정보취급자 별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ④개인정보취급자의 비밀번호를 일방향 암호화하여 저장하지 않은 사실(고시 제7조제2항), ⑤개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑥접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(양양군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하고 있지 않음 (고시 제5조제1항) ② 전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ③ 개인정보취급자 별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유하고 있음 (고시 제5조제4항) ④ 개인정보취급자의 비밀번호를 일방향 암호화하여 저장하지 않음 (고시 제7조제2항) ⑤ 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항) ⑥ 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여할 것

2) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-015호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 대전광역시청
대전광역시 서구 둔산로 100

의결연월일 2021. 1. 27.

주 문

1. 피심인 대전광역시청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 암호화 저장할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

4) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[7]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 5. 26.~5. 29.) 결과, 다음과 같은 사실을 확인하였다.

7) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실이 있다.

2) 피심인은 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실이 있다.

3) 피심인은 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실이 있다.

4) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보를 암호화하는 경우 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)
- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요

도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ②비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실(고시 제7조제5항), ③처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실(고시 제8조제1항), ④개인정보처리시스템의 접속기록을 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(대전광역시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ② 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않음 (고시 제7조제5항) ③ 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리함 (고시 제8조제1항) ④ 개인정보처리시스템의 접속기록을 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 암호화 저장할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

4) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　백 대 용　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　염 흥 열　(서 명)

위　　원　　이 희 정　(서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-016호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	오산시청 경기도 오산시 성호대로 141
의결연월일	2021. 1. 27.

주 문

1. 피심인 오산시청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보 처리 업무를 위탁하는 경우 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 한다.

나. 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

다. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

4) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

5) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

6) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

7) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

8) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

라. 가·나·다의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한

책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[8]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 6. 1.~6. 4.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 처리 업무를 위탁하면서 수탁자 공개를 소홀히 한 행위

8) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

피심인은 개인정보 처리 업무를 위탁하면서 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)*를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 하나, 일부를 공개하지 않은 사실이 있다.

*

나. 개인정보 처리 업무를 위탁하면서 수탁자 관리·감독을 소홀히 한 행위

피심인은 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보 처리 현황 점검 등 수탁자*가 개인정보를 안전하게 처리하는지를 감독하여야 하나, 이를 이행하지 않은 사실이 있다.

*

다. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인의 개인정보 보호책임자가 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않은 사실이 있다.

2) 피심인은 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실이 있다.

3) 피심인은 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실이 있다.

4) 피심인은 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실이 있다.

5) 피심인은 외부에서 관리자페이지에 접속할 경우 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실이 있다.

6) 피심인은 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실이 있다.

7) 피심인은 수행업무 및 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실이 있다.

8) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2021.1.22. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제26조제2항은 "제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다"고 규정하고 있다.

1)「개인정보 보호법 시행령」제28조제2항에 따르면 법 제26조제2항에서 "대통령령으로 정하는 방법"이란 위탁자가 위탁자의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하는 방법을 말한다.

2) 같은 법 시행령 제28조제3항에 따르면 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음의 어느 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하여야 한다; ①위탁자의 사업장 등의 보기 쉬운 장소에 게시하는 방법, ②관보나 위탁자의 사업자 등이 있는 시·도 이상의 지역을 주된 보급 지역으로 하는「신문 등의 진흥에 관한 법률」제2조제1호 가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법, ③같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법, ④재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

나.「개인정보 보호법」제26조제4항은 “위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다”고 규정하고 있다.

1) ‘개인정보보호 법령 및 지침·고시 해설’(행정안전부, 2016.12)에 따르면 위탁자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. 또한, 위탁자는 수탁자가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위수탁 계약(법 제26조제1항 각호에 따른 사항)의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다. 따라서 위탁자는 수탁자에 대해 정기적인 교육을 실시하는 외에 수탁자의 개인정보 처리현황 및 실태, 목적외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.

다.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2)「개인정보 보호법 시행령」제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보 보호책임자는 내부관리계획의 적정성과 실효성을 보장하기 위하여 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리하여야 한다. 내부관리계획의 이행 실태 점검·관리 결과에 따라 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다. (제4조제4항)

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)

- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보

처리시스템, 접근통제시스템, 인터넷홈페이지 등에 적용하여야 한다. 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 하며, 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다. (제5조제5항)

- 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(인증서, OTP 등)을 적용하여 정당한 접근 권한자임을 확인하는 등의 조치를 취하여야 한다. (제5조제6항)
- 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. 인터넷 구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (제6조제2항)
- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암호화하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)
- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보 처리 업무를 위탁하면서 수탁자 공개를 소홀히 한 행위 (법 제26조제2항)

피심인이 개인정보 처리 업무를 위탁하면서 일부 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하지 않은 사실은 「개인정보 보호법」 제26조제2항을 위반한 것이다.

나. 개인정보 처리 업무를 위탁하면서 수탁자에 대한 관리·감독을 소홀히 한 행위 (법 제26조제4항)

피심인이 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리현황 점검 등 수탁자가 안전하게 처리하는 감독하지 않은 사실은 「개인정보 보호법」 제26조제4항을 위반한 것이다.

다. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보 보호책임자가 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않은 사실(고시 제4조제4항), ②개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하지 않은 사실(고시 제5조제3항), ③안전한 비밀번호 작성규칙을 적용하지 않은 사실(고시 제5조제5항), ④계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실(고시 제5조제6항), ⑤외부에서 관리자페이지에 접속할 경우 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실(고시 제6조제2항), ⑥비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실(고시 제7조제5항), ⑦수행업무 및 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑧개인정보처리시스템의 접속기록을 점검하지 않은 사

실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(오산시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보처리 위탁 시 (공개)	§26②	§28②	개인정보 처리 업무를 위탁하는 개인정보처리자는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 하나, 일부를 공개하지 않음
개인정보처리 위탁 시 (관리·감독)	§26④		업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 하나, 이를 이행하지 않음
안전조치의무	§29	§30①	① 개인정보 보호책임자가 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않음 (고시 제4조제4항) ② 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ③ 안전한 비밀번호 작성규칙을 적용하지 않음 (고시 제5조제5항) ④ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않음 (고시 제5조제6항) ⑤ 외부에서 관리자페이지에 접속할 경우 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않음 (고시 제6조제2항) ⑥ 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않음 (고시 제7조제5항) ⑦ 필수정보 중 수행업무 및 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리함 (고시 제8조제1항) ⑧ 개인정보처리시스템의 접속기록을 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보 처리 업무를 위탁하는 경우 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 한다.

나. 피심인은 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

다. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

4) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

5) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

6) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

7) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

8) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

라. 피심인은 가·나·다의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제26조제2항, 제26조제4항, 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-017호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	옹진군청 인천광역시 미추홀구 매소홀로 120
의결연월일	2021. 1. 27.

주 문

1. 피심인 옹진군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보 수집·이용 동의를 받을 때, 필수고지사항(수집항목, 수집·이용목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

2) 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[9]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리

9) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

실태 현장 검사('20. 6. 2.~6. 5.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보를 수집하면서 필수 고지사항을 알리지 않은 행위

피심인은 개인정보를 수집하면서 필수 항목 4가지(개인정보의 수집·이용목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용)를 알리고 있지 않은 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보취급자별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유한 사실이 있다.

2) 피심인은 정보주체의 비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제15조제2항에 따르면 개인정보처리자는 개인정보 수집 동의를 받을 때에는 다음 사항을 정보주체에게 알려야 하며, 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다; ①개인정보의 수집·이용목적, ②수집하려는 개인정보의 항목, ③개인정보의 보유 및 이용기간, ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

나. 「개인정보 보호법」 제29조는 "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 '개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)' 등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수

행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리 내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체를 통하여 전달하는 경우에는 이를 암호화하여야 한다. 고유식별정보는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다. 비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다. 정보통신망이란 전기통시사업법 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다. (제7조제1항)

2. 위법성 판단

가. 개인정보를 수집하면서 필수고지사항을 알리지 않은 행위 (법 제15조제2항)

피심인이 정보주체로부터 개인정보를 수집하면서 필수 고지사항을 모두 알리지 않은 사실은 「개인정보 보호법」 제15조제2항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자 별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유하고 있는 사실(고시 제5조제4항), ②정보주체의 비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않은 사실(고시 제7조제1항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(옹진군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보 수집·이용(고지)	§15②	-	개인정보를 수집하면서 필수 고지 항목 4가지를 모두 알리지 않음
안전조치의무	§29	§30①	① 개인정보취급자 별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유하고 있음 (고시 제5조제4항) ② 정보주체의 비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않음 (고시 제7조제1항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보 수집·이용 동의를 받을 때, 필수고지사항(수집항목, 수집·이용목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받을 것

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

2) 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

다. 피심인은 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제15조제2항, 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-018호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	영덕군청 경상북도 영덕군 영덕읍 군청길 116
의결연월일	2021. 1. 27.

주 문

1. 피심인 영덕군청에 대해 다음과 같이 시정조치를 권고한다.

가. 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

4) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[10]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 6. 1.~6. 4.) 결과, 다음과 같은 사실을 확인하였다.

10) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

2. 행위 사실

가. 개인정보 처리 업무 위탁 시 수탁자 관리·감독을 소홀히 한 행위

피심인은 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자에 대한 교육 및 감독을 하지 않은 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실이 있다.

2) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실이 있다.

3) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 보관·관리하지 않거나, 일부 항목을 누락하여 보관·관리한 사실이 있다.

4) 피심인은 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제26조제4항은 “위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다”고 규정하고 있다.

1) ‘개인정보보호 법령 및 지침·고시 해설’(행정안전부, 2016.12)에 따르면 위탁자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. 또한, 위탁자는 수탁자가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위수탁 계약(법 제26조제1항 각호에 따른 사항)의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다. 따라서 위탁자는 수탁자에 대해 정기적인 교육을 실시하는 외에 수탁자의 개인정보 처리현황 및 실태, 목적외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.

나. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적

및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 '개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)', '개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 **한**다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후

에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보 처리업무 위탁 시 수탁자 관리·감독을 소홀히 한 행위 (법 제26조제4항)

피심인이 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자에 대한 교육 및 감독을 하지 않은 것은 「개인정보 보호법」 제26조제4항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실(고시 제5조제3항), ②개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ③개인정보취급자가 개인정보처리시스템에 접속한 기록을 보관·관리하지 않거나, 일부 항목을 누락 보관·관리한 사실(고시 제8조제1항), ④개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(영덕군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보 처리 위탁 시 관리·감독	§26④	-	업무 위탁으로 인하여 정보주체의 개인정보가 분실・도난・유출・위조・변조 또는 훼손되지 아니하도록 수탁자에 대한 교육 및 감독을 하지 않음
안전조치의무	§29	§30①	① 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않음 (고시 제5조제3항) ② 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유함 (고시 제5조제4항) ③ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 보관·관리하지 않거나, 일부 항목을 누락 보관 관리함 (고시 제8조제1항) ④ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

4) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 피심인은 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제26조제4항 및 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-019호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	삼척시청 강원도 삼척시 중앙로 296
의결연월일	2021. 1. 27.

주 문

1. 피심인 삼척시청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보 수집·이용 동의를 받을 때, 필수 고지 사항(수집항목, 수집·이용목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

2) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

3) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[11]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 6. 1.~6. 4.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보를 수집하면서 필수 고지사항을 알리지 않은 행위

피심인은 개인정보를 수집하면서 필수 항목 4가지(개인정보의 수집·이용목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용)를 알리지 않고 개인정보를 수집한 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 알리지 않고 개인정보를 수집한 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실이 있다.

2) 피심인은 외부에서 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실이 있다.

11) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

3) 피심인은 비밀번호 저장 시 안전한 암호화 알고리즘을 사용하여 저장하지 않은 사실이 있다.

4) 전체 또는 일부 항목이 누락된 접속기록을 보관·관리함

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021. 1.25. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제15조제2항에 따르면 개인정보처리자는 개인정보 수집 동의를 받을 때에는 다음 사항을 정보주체에게 알려야 하며, 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다; ①개인정보의 수집·이용목적, ②수집하려는 개인정보의 항목, ③개인정보의 보유 및 이용 기간, ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

나.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고

발생 에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷홈페이지 등에 적용하여야 한다. 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 하며, 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다. (제5조제5항)
- 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. 인터넷 구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (제6조제2항)
- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를

암호화하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

2. 위법성 판단

가. 개인정보를 수집하면서 필수고지사항을 알리지 않은 행위 (법 제15조제2항)

피심인이 정보주체로부터 개인정보를 수집하면서 필수 고지사항을 모두 알리지 않은 사실은 「개인정보 보호법」 제15조제2항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실(고시 제5조제5항), ②외부에서 개인정보처리시스템에 접속할 경우 가상사설망

또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실(고시 제6조제2항), ③비밀번호 저장 시, 취약한 일방향 암호화 알고리즘을 사용하여 저장한 사실(고시 제7조제5항), ④전체 또는 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(삼척시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보 수집·이용 (고지)	§15②	-	개인정보처리자는 개인정보 수집·이용 동의를 받을 때, 필수 고지사항("동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용")을 알리지 않음
안전조치의무	§29	§30①	① 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않음 (고시 제5조제5항) ② 외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않음 (고시 제6조제2항) ③ 비밀번호 저장 시, 취약한 일방향 암호화 알고리즘을 사용하여 저장함 (고시 5제7조제5항) ④ 전체 또는 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보 수집·이용 동의를 받을 때, 필수 고지사항(수집항목, 수집·이용목적, 보유·이용 기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

2) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

3) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

다. 피심인은 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제15조제2항, 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-020호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	안산시청 경기도 안산시 단원구 화랑로 387
의결연월일	2021. 1. 27.

주 문

1. 피심인 안산시청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[12]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보

12) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

관리실태 현장 검사('20. 6. 8.~6. 11.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실이 있다.

2) 피심인은 현수막지정게시대 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실이 있다.

3) 피심인은 개인정보취급자별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실이 있다.

4) 피심인은 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동적으로 시스템 접속이 차단되도록 하지 않은 사실이 있다.

5) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실이 있다.

6) 피심인은 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)
- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을

발급하는 경우 개인정보취급자별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다. 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속의 차단을 의미하며, 업무용 컴퓨터의 화면 보호기 등은 접속차단에 해당하지 않는다. 개인정보취급자가 일정시간 이상 업무처리를 하지 않아 개인정보처리시스템에 접속이 차단된 이후, 다시 접속하조가 할 때에도 최초의 로그인과 동일한 방법으로 접속하여야 한다. (제6조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상

행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실(고시 제5조제3항), ③개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ④개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보 취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동적으로 시스템 접속이 차단되도록 하지 않은 사실(고시 제6조제5항), ⑤개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑥개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(안산시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않음 (고시 제5조제3항) ③ 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유함 (고시 제5조제4항) ④ 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보 취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동적으로 시스템 접속이 차단되도록 하지 않았음 (고시 제6조제5항) ⑤ 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항) ⑥ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-021호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	금천구청 서울특별시 금천구 시흥대로 73길 70
의결연월일	2021. 1. 27.

주 문

1. 피심인 금천구청에 대해 다음과 같이 시정조치를 권고한다.

가. 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.

나. 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

다. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 암호화 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

라. 가·나·다의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[13]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 6. 8.~6. 11.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 목적달성 후 개인정보를 파기하지 않은 행위

피심인은 보유기간의 경과, 개인정보의 처리 목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기해야 하나, 5년 지난 개인정보를 파기하지 않은 사실이 있다.

나. 개인정보 처리업무 위탁 시 수탁자 관리·감독을 소홀히 한 행위

피심인이 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 하나, 이를 이행하지 않은 사실이 있다.

다. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실이 있다.

13) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

2) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실이 있다.

3) 피심인은 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실이 있다.

4) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제21조제1항은 "개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다."고 규정하고 있다.

1)「개인정보 보호법 시행령」제16조제1항에 따르면 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음의 구분에 따른 방법으로 하여야 한다; ①전자적 파일 형태인 경우 : 복원이 불가능한 방법으로 영구 삭제, ②그 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 파쇄 또는 소각

2) ‘개인정보보호 법령 및 지침·고시 해설’(행정안전부, 2016.12)에 따르면 개인정보처리자는 개인정보가 불필요하게 되었을 때에는 지체없이 해당 개인정보를 파기해야 한다. “개인정보가 불필요하게 되었을 때”란 개인정보의 처리 목적이 달성되었거나, 해당 서비스의 폐지, 사업이 종료된 경우 등이 포함된다. 따라서 개인정보처리자는 처리목적이 달성되거나 해당 서비스 및 사업이 종료된 경우, 정당한 사유가 없는 한 5일 이내에 개인정보를 파기하여야 한다.(표준지침 제10조제1항) 개인정보의 보존필요성이 있는지 여부는 개관적으로 판단해야 하며, 자의적으로 해석해서는 안된다.

나. 「개인정보 보호법」 제26조제4항은 “위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다”고 규정하고 있다.

1) ‘개인정보보호 법령 및 지침·고시 해설’(행정안전부, 2016.12)에 따르면 위탁자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. 또한, 위탁자는 수탁자가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위수탁 계약(법 제26조제1항 각호에 따른 사항)의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다. 따라서 위탁자는 수탁자에 대해 정기적인 교육을 실시하는 외에 수탁자의 개인정보 처리현황 및 실태, 목적외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.

다.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2)「개인정보 보호법 시행령」제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)
- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암

호화 하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

2. 위법성 판단

가. 목적달성 후 개인정보를 파기하지 않은 행위 (제21조제1항)

피심인은 보유기간의 경과, 개인정보의 처리 목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기해야 하나 개인정보를 파기하지 않은 사실은 「개인정보 보호법」 제21조제1항을 위반한 것이다.

나. 개인정보 처리업무 위탁 시 수탁자 관리·감독을 소홀히 한 행위 (법 제26조제4항)

피심인이 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·

변조 또는 훼손되지 아니하도록 개인정보 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 하나, 이를 이행하지 않은 사실은 「개인정보 보호법」 제26조제4항을 위반한 것이다.

다. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실(고시 제5조제3항), ②개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ③비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장하지 않은 사실(고시 제7조제5항), ④개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(금천구청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보 미파기	§21①	§16	보유기간이 경과한 개인정보 미파기
수탁사 관리·감독	§26④	§28⑥	수탁자에 대한 감독 미이행
안전조치의무	§29	§30①	① 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않음 (고시 제5조제3항) ② 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유함 (고시 제5조제4항) ③ 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않음 (고시 제7조제5항) ④ 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.

나. 피심인은 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

다. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관 할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자 별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 암호화 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

라. 피심인은 가·나·다의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제21조제1항, 제26조제4항 및 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-022호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 강원도청
강원도 춘천시 중앙로 1(봉의동)

의결연월일 2021. 1. 27.

주 문

1. 피심인 강원도청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리 할 것

2) 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 기초자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[14]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 6. 8~6. 11.) 결과, 다음과 같은 사실을 확인하였다.

14) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보 보호책임자가 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않은 사실이 있다.

2) 피심인은 수행 업무(수정·다운로드)가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 ’21.1.25 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보의 안전한 처리를 위한 내부관리계획의 수립·시행(제1호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보 보호책임자는 내부관리계획의 적정성과 실효성을 보장하기 위하여 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리하여야 한다. 내부관리계획의 이행 실태 점검·관리 결과에 따라 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다. (제4조제4항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보 보호책임자를 통해 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않은 사실(고시 제4조제4항), ②수행업무(수정·다운로드)가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실(고시 제8조제1항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(강원도청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보 보호책임자가 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않음 (고시 제4조제4항) ② 수행업무(수정·다운로드)가 누락된 개인정보취급자의 접속기록을 보관·관리함 (고시 제8조제1항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행 실태를 연 1회 이상 점검·관리할 것

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯

하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-023호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	칠곡군청 경북 칠곡군 왜관읍 군청1길 80
의결연월일	2021. 1. 27.

주 문

1. 피심인 칠곡군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자 별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

2) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 기초자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[15]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 8.~6. 11.) 결과, 다음과 같은 사실을 확인하였다.

15) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실이 있다.

2) 피심인은 개인정보취급자의 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실이 있다.

3) 피심인은 개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 접속기록을 보관·관리한 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 '21.1.25. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 '개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)', '개인정보침해사

고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동

안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ②개인정보취급자의 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실(고시 제7조제5항), ③개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 접속기록을 보관·관리한 사실(고시 제8조제1항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(칠곡군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유됨 (고시 제5조제4항) ② 개인정보취급자의 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않음 (고시 제7조제5항) ③ 개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 접속기록을 보관·관리함 (고시 제8조제1항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적

보호조치를 하여야 한다.

1) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

2) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-024호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 태백시청
강원도 태백시 태붐로 21

의결연월일 2021. 1. 27.

주 문

1. 피심인 태백시청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

3) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 기초자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[16]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 9.~6. 12.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

16) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

1) 피심인은 개인정보취급자가 변경되었을 경우, 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실이 있다.

2) 피심인은 외부에서 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실이 있다.

3) 피심인은 비밀번호 저장 시, 안전한 암호화 알고리즘을 사용하지 않은 사실이 있다.

4) 피심인은 개인정보취급자의 접속기록을 보관·관리하지 않거나 일부 누락된 접속기록을 보관·관리한 사실이 있다.

5) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는

암호화 기술의 적용 또는 이에 상응하는 조치(제3호)', '개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)
- 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. 인터넷 구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (제6조제2항)
- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자가 변경되었을 경우, 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실(고시 제6조제2항), ③비밀번호 저장 시, 안전한 암호화 알고리즘을 사용하지 않은 사실(고시 제7조제5항), ④개인정보취급자의 접속기록을 보관·관리하지 않거나, 일부 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑤개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(태백시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보취급자가 변경되었을 경우, 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않음 (고시 제6조제2항) ③ 비밀번호 저장 시, 안전한 암호화 알고리즘을 사용하지 않음 (고시 제7조제5항) ④ 개인정보취급자의 접속기록을 보관·관리하지 않거나, 일부 누락된 접속기록을 보관·관리함 (고시 제8조제1항) ⑤ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인

정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

3) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-025호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 양구군청
강원도 양구군 양구읍 관공서로 38

의결연월일 2021. 1. 27.

주 문

1. 피심인 양구군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보 수집·이용 동의를 받을 때, 필수 고지사항(수집항목, 수집·이용목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

4) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[17]는「개인정보 보호법」위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 15.~6. 18.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보를 수집하면서 필수 고지사항을 알리지 않은 행위

피심인은 개인정보를 수집하면서 필수 항목 4가지(개인정보의 수집·이용목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용)를 알리지 않고 개인정보를 수집한 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실이 있다.

2) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실이 있다.

3) 피심인 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실이 있다.

4) 피심인은 상비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않은 사실이 있다.

---

17) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

5) 피심인은 개인정보취급자가 접속한 기록을 보관·관리하지 않은 사실이 있고, 상하수도요금관리시스템에서는 수행업무 중 다운로드 기록 누락된 접속기록을 보관·관리한 사실이 있다.

6) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021. 1.25. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제15조제2항에 따르면 개인정보처리자는 개인정보 수집 동의를 받을 때에는 다음 사항을 정보주체에게 알려야 하며, 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다; ①개인정보의 수집·이용목적, ②수집하려는 개인정보의 항목, ③개인정보의 보유 및 이용 기간, ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

나. 「개인정보 보호법」 제29조는 "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(인증서, OTP 등)을 적용하여 정

당한 접근 권한 자임을 확인하는 등의 조치를 취하여야 한다. (제5조제6항)

- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다. (제7조제2항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리

시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보를 수집하면서 필수고지사항을 알리지 않은 행위 (법 제15조제2항)

피심인이 정보주체로부터 개인정보를 수집하면서 필수 고지사항을 모두 알리지 않은 사실은 「개인정보 보호법」 제15조제2항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실(고시 제5조제3항), ②개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ③계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실(고시 제5조제6항), ④비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않은 사실(고시 제7조제2항), ⑤개인정보취급자가 개인정보처리시스템에 접속한 기록을 누락 없이 보관·관리하지 않은 사실(고시 제8조제1항), ⑥개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(양구군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보 수집·이용(고지)	§15②	-	개인정보 수집·이용 동의를 받을 때, 필수 고지사항을 알리지 않음
안전조치의무	§29	§30①	① 개인정보처리시스템의 접근 권한 등록, 변경, 말소에 대한 내역을 기록하지 않음 (고시 제5조제3항) ② 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유함 (고시 제5조제4항) ③ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않았음 (고시 제5조제6항) ④ 비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않음 (고시 제7조제2항) ⑤ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 누락 없이 보관·관리하지 않음 (고시 제8조제1항) ⑥ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보 수집·이용 동의를 받을 때, 필수 고지사항(수집항목, 수집·이용목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급할 것

3) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

4) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 피심인은 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제15조제2항, 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-026호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	강남구청 서울특별시 강남구 학동로 426(삼성동)
의결연월일	2021. 1. 27.

주 문

1. 피심인 강남구청에 대해 다음과 같이 시정조치를 권고한다.

가. 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 비밀번호를 안전한 암호화 알고리즘으로 일방향 암호화하여 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[18]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 15.~6. 18.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 처리업무 위탁 시 수탁자 관리·감독을 소홀히 한 행위

피심인은 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 하나, 이를 이행하지 않은 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실이 있다.

2) 피심인은 개인정보취급자별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실이 있다.

3) 피심인은 비밀번호를 안전한 암호알고리즘으로 일방향 암호화하여 저장하지 않은 사실이 있다.

4) 피심인은 개인정보취급자가 일부 접속기록 항목을 누락하여 보관·관리한 사실이 있다.

---

18) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

5) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제26조제4항은 “위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다”고 규정하고 있다.

1) ‘개인정보보호 법령 및 지침·고시 해설’(행정안전부, 2016.12)에 따르면 위탁자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. 또한, 위탁자는 수탁자가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위수탁 계약(법 제26조제1항 각호에 따른 사항)의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다. 따라서 위탁자는 수탁자에 대해 정기적인 교육을 실시하는 외에 수탁자의 개인정보 처리현황 및 실태, 목적외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.

나. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·

위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 '개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)', '개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야

한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다. (제7조제2항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)
- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정

보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보 처리업무 위탁 시 수탁자 관리·감독을 소홀히 한 행위 (법 제26조제4항)

피심인이 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하지 않은 사실은「개인정보 보호법」 제26조제4항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하지 않은 사실(고시 제5조제3항), ②개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ③비밀번호 저장시 안전한 암호화 알고리즘으로 일방향 암호화 하지 않은 사실(고시 제7조제2항), ④개인정보취급자가 개인정보처리시스템에 접속한 기록을 누락 없이 보관·관리하지 않은 사실(고시 제8조제1항), ⑤개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(강남구청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
수탁자 관리·감독	§26④		개인정보 처리 업무 위탁 시 수탁자의 개인정보 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지 관리· 감독하지 않음
안전조치의무	§29	§30①	① 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록하지 않음 (고시 제5조제3항) ② 개인정보취급자별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유하여 사용함(고시 제5조제4항) ③ 비밀번호 저장시 안전한 암호화 알고리즘으로 일방향 암호화 하지 않음 (고시 제7조제2항) ④ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 누락 없이 보관·관리하지 않음 (고시 제8조제1항) ⑤ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 비밀번호를 안전한 암호화 알고리즘으로 일방향 암호화하여 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 피심인은 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 3날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의「개인정보 보호법」제26조제4항 및 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-027호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 성주군청
경북 성주군 성주읍 성주로 3200

의결연월일 2021. 1. 27.

주 문

1. 피심인 성주군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

2) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[19]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 15.~6. 18.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

19) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

1) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자 계정이 다른 개인정보취급자와 공유된 사실이 있다.

2) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2)「개인정보 보호법 시행령」제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을

발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ②개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(성주군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보취급자별로 사용자계정을 발급하지 않고, 다른 개인정보취급자와 공유하여 사용함 (고시 제5조제4항) ② 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

2) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을

실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-028호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	영월군청 강원도 영월군 영월읍 하송로 64
의결연월일	2021. 1. 27.

주 문

1. 피심인 영월군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행 실태를 연1회 이상으로 점검·관리할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관 할 것

3) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나, 안전한 인증수단을 적용할 것

4) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[20]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 15.~6. 18.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

20) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보처리시스템에 대해 연 1회 이상 내부관리계획의 이행 실태를 점검·관리하지 않은 사실이 있다.

2) 피심인은 개인정보취급자의 접근권한 변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실이 있다.

3) 피심인은 외부에서 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실이 있다.

4) 피심인은 비밀번호를 안전한 알고리즘으로 일방향 암호화하여 저장하지 않은 사실이 있다.

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실이 있다.

6) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.20. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보의 안전한 처리를 위한 내부관리계획의 수립·시행(제1호)’, ‘개인정보에 대한 접근 통제 및 접근권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보 보호책임자는 내부관리계획의 적정성과 실효성을 보장하기 위하여 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리하여야 한다. 내부관리계획의 이행 실태 점검·관리 결과에 따라 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다. (제4조제4항)
- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적

으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)

- 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. 인터넷 구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (제6조제2항)

- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록

및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보처리시스템에 대해 연 1회 이상 내부관리계획의 이행 실태를 점검·관리하지 않은 사실(고시 제4조제4항), ②개인정보취급자의 접근권한 변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ③외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실(고시 제6조제2항), ④비밀번호를 안전한 알고리즘으로 암호화하여 저장하지 않은 사실(고시 제7조제5항), ⑤개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑥개인정보처리시스

템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(영월군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보처리시스템에 대해 연 1회 이상 내부 관리계획의 이행 실태를 점검·관리하지 않음 (고시 제4조제4항) ② 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록하지 않음 (고시 제5조제3항) ③ 외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않음 (고시 제6조제2항) ④ 비밀번호를 안전한 알고리즘으로 암호화하여 저장하지 않음 (고시 제7조제5항) ⑤ 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항) ⑥ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속

하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

4) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

6) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-029호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	달성군청 대구광역시 달성군 논공읍 달성군청로 33
의결연월일	2021. 1. 27.

주 문

1. 피심인 달성군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보 수집·이용 동의를 받을 때, 필수고지사항(수집항목, 수집·이용 목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리할 것

2) 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여할 것

3) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

4) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

5) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

6) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

7) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

8) 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 할 것

9) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리 할 것

10) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[21]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 7. 6.~7. 9.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보를 수집하면서 필수 고지사항을 알리지 않은 행위

피심인은 개인정보를 수집하면서 필수항목 4가지(개인정보의 수집·이용목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용)를 알리지 않고 개인정보를 수집한 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 연 1회 이상 내부관리계획의 이행 실태를 점검·관리하지 않은 사실이 있다.

---

21) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

2) 피심인은 대한 접근 권한을 업무 담당자에 따라 차등 부여하지 않은 사실이 있다.

3) 피심인은 전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실이 있다.

4) 피심인은 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음

5) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실이 있다.

6) 피심인은 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실이 있다.

7) 피심인은 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실이 있다.

8) 피심인은 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 기술적 조치를 취하지 않은 사실이 있다.

9) 피심인은 개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 접속기록을 보관·관리한 사실이 있다.

10) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.25. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제15조제2항에 따르면 개인정보처리자는 개인정보 수집 동의를 받을 때에는 다음 사항을 정보주체에게 알려야 하며, 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다; ①개인정보의 수집·이용목적, ②수집하려는 개인정보의 항목, ③개인정보의 보유 및 이용 기간, ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

나. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보의 안전한 처리를 위한 내부관리계획의 수립·시행(제1호)’, ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보 보호책임자는 내부관리계획의 적정성과 실효성을 보장하기 위하여 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리하여야 한다. 내부관리계획의 이행 실태 점검·관리 결과에 따라 적절한 조치를 취하여야 하며, 중대한

영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다. (제4조제4항)

- 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행 목적에 따라 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 접근통제를 위한 안전조치를 취해야 한다. 특히, 개인정보처리시스템의 데이터베이스(DB)에 대한 직접적인 접근은 데이터베이스 운영·관리자에 한정하는 등의 안전조치를 적용할 필요성이 있다. (제5조제1항)
- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)
- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)
- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷홈페이지 등에 적용하여야 한다. 비밀

번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 하며, 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다. (제5조제5항)

- 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(인증서, OTP 등)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치를 취하여야 한다. (제5조제6항)

- 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다. 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속의 차단을 의미하며, 업무용 컴퓨터의 화면 보호기 등은 접속차단에 해당하지 않는다. 개인정보취급자가 일정시간 이상 업무처리를 하지 않아 개인정보처리시스템에 접속이 차단된 이후, 다시 접속하고자 할 때에도 최초 로그인과 동일한 방법으로 접속하여야 한다. (제6조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이

후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보를 수집하면서 필수고지사항을 알리지 않은 행위 (법 제15조제2항)

피심인이 정보주체로부터 개인정보를 수집하면서 필수 고지사항을 모두 알리지 않은 사실은 「개인정보 보호법」 제15조제2항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보 보호책임자가 연 1회 이상 내부관리계획의 이행 실태를 점검·관리하지 않은 사실(고시 제4조제4항), ②개인정보처리시스템에 대한 접근권한을 업무 담당자에 따라 차등 부여하지 않은 사실(고시 제5조제1항, ③전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ④개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ⑤개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ⑥안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실(고시 제5조제5항), ⑦계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실(고시 제5조제6항), ⑧개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 기술적 조치를 취하지 않은 사실(고시 제6조제5항), ⑨개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑩개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(달성군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보 수집·이용	§15②	-	개인정보 수집 시 필수 네가지 항목을 누락하고 동의를 받음
안전조치의무	§29	§30①	① 개인정보 보호책임자가 연 1회 이상으로 내부관리계획의 이행 실태를 점검·관리하지 않음 (고시 제4조제4항) ② 개인정보처리시스템에 대한 접근 권한을 업무 담당자에 따라 차등 부여하지 않음 (고시 제5조제1항) ③ 전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ④ 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ⑤ 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유됨 (고시 제5조제4항) ⑥ 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않음 (고시 제5조제5항) ⑦ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않음 (고시 제5조제6항) ⑧ 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 기술적 조치를 취하지 않음 (고시 제6조제5항) ⑨ 개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 접속기록을 보관·관리함 (고시 제8조제1항) ⑩ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보 수집·이용 동의를 받을 때, 필수 고지사항(수집항목, 수집·이용목적, 보유·이용기간, 거부 시 불이익 사항)을 모두 알리고 동의를 받아야 한다.

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행실태를 연1회 이상으로 점검·관리할 것

2) 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여할 것

3) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

4) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

5) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

6) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

7) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

8) 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 할 것

9) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

10) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

다. 피심인은 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제15조제2항, 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-030호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	영주시청 경북 영주시 시청로 1
의결연월일	2021. 1. 27.

주 문

1. 피심인 영주시청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

5) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

6) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

7) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

8) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은「개인정보 보호법」제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로「지방자치법」제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[22]는「개인정보 보호법」위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 22.~6. 25.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 시 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하지 않은 사실이 있다.

2) 피심인은 시 접근 권한 중 '변경, 말소'에 대한 내역을 기록하지 않은 사실이 있다.

3) 피심인은 시 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실이 있다.

4) 피심인은 안전한 비밀번호 작성규칙은 수립하였으나,이를 적용하지 않은 사실이 있다.

5) 피심인은 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하는 등 필요한 기술적 조치를 하지 않은 사실이 있다.

6) 피심인은 비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않은 사실이 있다.

7) 피심인은 개인정보취급자가 접속한 기록을 보관·관리하지 않거나, 일부를 누락하여 관리한 사실이 있다.

---

22) 2020. 8. 5. 시행된 개정「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

8) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리

시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)
- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷홈페이지 등에 적용하여야 한다. 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 하며, 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다. (제5조제5항)
- 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보·비

밀번호 입력과 동시에 추가적인 인증수단(인증서, OTP 등)을 적용하여 정당한 접근 권한자임을 확인하는 등의 조치를 취하여야 한다. (제5조제6항)

- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다. (제7조제2항)
- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)
- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고

적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ③개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ④안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실(고시 제5조제5항), ⑤계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실(고시 제5조제6항), ⑥비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않은 사실(고시 제7조제2항), ⑦개인정보취급자의 접속기록 항목 중 전체 또는 일부를 누락한 상태로 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑧개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(영주시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ③ 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유됨 (고시 제5조제4항) ④ 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않음 (고시 제5조제5항) ⑤ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않음 (고시 제5조제6항) ⑥ 비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않음 (고시 제7조제2항) ⑦ 개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 접속기록을 보관·관리함 (고시 제8조제1항) ⑧ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않았음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

5) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

6) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

7) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

8) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-031호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	동두천시청 경기도 동두천시 방죽로 23
의결연월일	2021. 1. 27.

주 문

1. 피심인 동두천시청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관 할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

4) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[23]는「개인정보 보호법」위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 22.~6. 25.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하지 않은 사실이 있다.

2) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유된 사실이 있다.

3) 피심인은 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실이 있다.

4) 피심인은 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실이 있다.

5) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.22.의견을 제출하였다.

---

23) 2020. 8. 5. 시행된 개정「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보

취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷홈페이지 등에 적용하여야 한다. 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 하며, 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다. (제5조제5항)

- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·

감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음(고시 제5조제3항), ②개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ③안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않은 사실(고시 제5조제5항), ④안전하지 않은 알고리즘으로 암호화(고시 제7조제5항), ⑤개인정보취급자의 접속기록 항목 중 전체 또는 일부를 누락한 상태로 접속기록을 보관·관리한 사실(고시 제8조제1항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(동두천시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ② 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유됨 (고시 제5조제4항) ③ 안전한 비밀번호 작성규칙은 수립하였으나 이를 적용하지 않음 (고시 제5조제5항) ④ 안전하지 않은 알고리즘으로 암호화 (고시 제7조제5항) ⑤ 개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 접속기록을 보관·관리함 (고시 제8조제1항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하‘고 3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용할 것

4) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

5) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 “「개인정보 보호법」 위반에 따른 행정처분 통지”를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하

여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-032호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 화천군청
강원도 화천군 화천새싹길 45

의결연월일 2021. 1. 27.

주 문

1. 피심인 화천군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

4) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

5) 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나, 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

6) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

7) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

8) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은「개인정보 보호법」제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로「지방자치법」제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[24]는「개인정보 보호법」위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 7. 6.~7. 9.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실이 있다.

2) 피심인은 개인정보취급자의 접근권한 변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실이 있다.

3) 피심인은 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실이 있다.

4) 피심인은 외부에서 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실이 있다.

5) 피심인은 정보주체의비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않은 사실이 있다.

6) 피심인은 개인정보취급자 및 정보주체의 비밀번호를 일방향 암호화하여 저장하지 않은 사실이 있다.

7) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부

24) 2020. 8. 5. 시행된 개정「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

항목이 누락된 접속기록을 보관·관리한 사실이 있다.

8) 피심인은 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.25.의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 「개인정보 보호법」 제29조는 "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 '개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)', '개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인

정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)
- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(인증서, OTP 등)을 적용하여 정당한 접근 권한자임을 확인하는 등의 조치를 취하여야 한다. (제5조제6항)
- 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. 인터넷 구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (제6조제2항)

- 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체를 통하여 전달하는 경우에는 이를 암호화 하여야 한다. 고유식별정보는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다. 비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다. 정보통신망이란 전기통시사업법 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다. (제7조제1항)
- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다. (제7조제2항)
- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중

요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②개인정보취급자의 접근권한 변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ③비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취

하지 않은 사실(고시 제5조제6항), ④외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실(고시 제6조제2항), ⑤정보주체의 비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않은 사실(고시 제7조제1항), ⑥개인정보취급자 및 정보주체의 비밀번호를 일방향 암호화하여 저장하지 않은 사실(고시 제7조제2항), ⑦개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑧개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(화천군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 전보 또는 퇴직 등 인사이동으로 인해 개인정보취급자가 변경되었을 때 이에 대한 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 개인정보취급자의 접근권한 변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ③ 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않음 (고시 제5조제6항) ④ 외부에서 개인정보처리시스템에 접속할 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않음 (고시 제6조제2항) ⑤ 정보주체의 비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않음 (고시 제7조제1항) ⑥ 개인정보취급자 및 정보주체의 비밀번호를 일방향 암호화하여 저장하지 않음 (고시 제7조제2항) ⑦ 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항) ⑧ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

4) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용할 것

5) 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나, 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

6) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

7) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

8) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상'으로 정기적인 교육을

실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-033호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	서울특별시중구청 서울특별시 중구 창경궁로 17
의결연월일	2021. 1. 27.

주 문

1. 피심인 서울특별시중구청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관 할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 비밀번호를 저장하는 경우 일방향 암호화 저장할 것

5) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

6) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

7) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[25]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 22.~6. 25.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 전보 또는 퇴직 등 인사이동으로 개인정보취급자가 변경되었음에도 접근권한을 변경 또는 말소하지 않은 사실이 있다.

2) 피심인은 개인정보취급자의 접근권한 말소에 대한 내역을 기록·보관하고 있지 않은 사실이 있다.

3) 피심인은 사용자계정을 개인정보취급자별로 발급하지 않고 다른 개인정보취급자와 공유된 사실이 있다.

4) 피심인은 개인정보취급자의 비밀번호 저장 시 일방향 암호화를 적용하지 않은 사실이 있다.

5) 피심인은 개인정보취급자 정보주체의 비밀번호를 안전한 암호화 알고리즘을 사용하여 암호화하지 않은 사실이 있다.

6) 피심인은 개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 보관·관리한 사실이 있다.

7) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

25) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.25.의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)
- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)
- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다. (제7조제2항)

- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제7조제5항)
- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)
- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내

부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①전보 또는 퇴직 등 인사이동으로 개인정보취급자가 변경되었음에도 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②개인정보취급자의 접근권한 말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ③사용자계정을 개인정보취급자 별로 발급하지 않고 다른 개인정보취급자와 공유됨(고시 제5조제4항), ④개인정보취급자의 비밀번호 저장 시 일방향 암호화를 적용하지 않은 사실(고시 제7조제2항), ⑤개인정보취급자(대형 생활폐기물 수거 업무용) 및 정보주체의 비밀번호를 안전한 암호화 알고리즘을 사용하여 암호화하지 않은 사실(고시 제7조제5항), ⑥개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 보관·관리한 사실(고시 제8조제1항), ⑦개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항 관련)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(서울중구청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 전보 또는 퇴직 등 인사이동으로 개인정보취급자가 변경되었음에도 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 개인정보취급자의 접근권한 말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ③ 사용자계정을 개인정보취급자 별로 발급하지 않고 다른 개인정보취급자와 공유됨 (고시 제5조제4항) ④ 개인정보취급자의 비밀번호 저장 시 일방향 암호화를 적용하지 않음 (고시 제7조제2항)

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
			⑤ 개인정보취급자(대형 생활 폐기물 수거 업무용) 및 정보주체의 비밀번호를 안전한 암호화 알고리즘을 사용하여 암호화하지 않음 (고시 제7조제5항) ⑥ 개인정보취급자의 접속기록 항목 중 일부를 누락한 상태로 보관·관리함 (고시 제8조제1항) ⑦ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않았음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

3) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

4) 비밀번호를 저장하는 경우 일방향 암호화 저장할 것

5) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

6) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

7) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-034호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	철원군청 강원도 철원군 갈말읍 삼부연로 51
의결연월일	2021. 1. 27.

주 문

1. 피심인 철원군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관 할 것

2) 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나, 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

3) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[26]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 6. 22.~6. 25.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

26) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

1) 피심인은 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하지 않은 사실이 있다.

2) 피심인은 비밀번호를 정보통신망을 통하여 송신 시 암호화하지 않은 사실이 있다.

3) 피심인은 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실이 있다.

4) 피심인은 아이디, 수행업무, 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실이 있다.

5) 피심인은 접속기록을 월 1회 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.21. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1)「개인정보 보호법 시행령」제30조제1항은 ‘개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)’, ‘개인정보를 안전하게 저장·전송할 수 있는

암호화 기술의 적용 또는 이에 상응하는 조치(제3호)', '개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)

- 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체를 통하여 전달하는 경우에는 이를 암호화하여야 한다. 고유식별정보는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다. 비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다. 정보통신망이란 전기통시사업법 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다. (제7조제1항)

- 개인정보처리자는 개인정보를 암호화하는 경우에는 안전한 암호화 알고리즘으로 암호화하여 저장하여야 한다. 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여야 한다. (제

7조제5항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)
- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않은 사실(고시 제5조제3항), ②비밀번호를 정보통신망을 통하여 송신 시 암호화 하지 않은 사실(고시 제7조제1항), ③비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않은 사실(고시 제7조제5항), ④아이디, 수행업무, 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑤개인정보처리시스템의 접속기록을 월 1회 점검하지 않은 사실(고시 제8조제2항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(철원군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ② 비밀번호를 정보통신망을 통하여 송신 시 암호화 하지 않음 (고시 제7조제1항) ③ 비밀번호를 안전한 암호알고리즘으로 암호화하여 저장하지 않음 (고시 제7조제5항) ④ 아이디, 수행업무, 처리한 정보주체 정보가 누락된 개인정보취급자의 접속기록을 보관·관리함 (고시 제8조제1항) ⑤ 개인정보처리시스템의 접속기록을 월 1회 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인

정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나, 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

3) 비밀번호를 안전한 암호화 알고리즘으로 암호화하여 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의「개인정보 보호법」제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2021-002-035호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 의성군청
경북 의성군 의성읍 군청길 31

의결연월일 2021. 1. 27.

주 문

1. 피심인 의성군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관 할 것

2) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

3) 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나, 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은「개인정보 보호법」제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로「지방자치법」제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[27]는「개인정보 보호법」위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 29.~7. 2.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

27) 2020. 8. 5. 시행된 개정「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보취급자의 접근권한 변경·말소에 대한 내역을 기록·보관하지 않은 사실이 있다.

2) 피심인은 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실이 있다.

3) 피심인은 정보주체의 비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않은 사실이 있다.

4) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실이 있다.

5) 피심인은 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실이 있다. (’20. 6월부터 월 1회 점검)

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.25. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등

대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 '개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)', '개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)

- 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자 계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(인증서, OTP 등)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치를 취하여야 한다. (제5조제6항)

- 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체를 통하여 전달하는 경우에는 이를 암호화하여야 한다. 고유식별정보는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록

번호를 말한다. 비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다. 정보통신망이란 전기통시사업법 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다. (제7조제1항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보취급자의 접근권한 변경·말소에 대한 내역을 기록·보관하지 않은 사실(고시 제5조제3항), ②비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않은 사실(고시 제5조제6항), ③정보주체의 비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않은 사실(고시 제7조제1항), ④개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항), 5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(의성군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보취급자의 접근권한 변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ② 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하지 않음 (고시 제5조제6항) ③ 정보주체의 비밀번호를 정보통신망을 통해 송신하면서 이를 암호화하지 않음 (고시 제7조제1항) ④ 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항) ⑤ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관할 것

2) 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 할 것

3) 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나, 보조저장매체를 통하여 전달하는 경우에는 이를 암호화할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-036호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	전남곡성군청 전라남도 곡성군 곡성읍 군청로 50
의결연월일	2021. 1. 27.

주 문

1. 피심인 전남곡성군청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[28]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 6. 29.~7. 2.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

28) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 접근 권한을 변경 또는 말소하지 않은 사실이 있다.

2) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실이 있다.

3) 피심인은 비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않은 사실이 있다.

4) 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실이 있다.

5) 피심인은 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으나, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 '개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)', '개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 조직 내 임직원의 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여 인가되지 않는 자의 접근을 차단하여야 한다. (제5조제2항)

- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)

- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀

번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다. (제7조제2항)

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회

수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않은 사실(고시 제5조제2항), ②개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ③비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않은 사실(고시 제7조제2항), ④개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항), ⑤개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(곡성군청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하지 않음 (고시 제5조제2항) ② 개인정보취급자 별로 사용자계정을 발급하지 않고, 사용자계정을 다른 개인정보취급자와 공유함 (고시 제5조제4항) ③ 비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않음 (고시 제7조제2항) ④ 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항) ⑤ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템에 대한 접근권한을 변경 또는 말소할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

4) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

5) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

나. 피심인은 가의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의「개인정보 보호법」제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-037호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	성동구청 서울시 성동구 고산자로 270
의결연월일	2021. 1. 27.

주 문

1. 피심인 성동구청에 대해 다음과 같이 시정조치를 권고한다.

가. 개인정보 처리 업무를 위탁하는 때에는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 한다.

나. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

다. 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[29]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리 실태 현장 검사('20. 6. 29.~7. 2.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

29) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

가. 개인정보 처리 업무를 위탁하면서 수탁자 공개를 소홀히 한 행위

피심인이 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 하나, 일부*를 공개하지 않은 사실이 있다.

나. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 비밀번호를 저장 시 일방향 암호화를 적용하지 않은 사실이 있다.

2) 피심인은 개인정보 취급자의 접속기록 보관ㆍ관리를 소홀히 한 사실이 있다.

다. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.25. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제26조제2항은 “제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제28조제2항에 따르면 법 제26조제2항에서 “대통령령으로 정하는 방법”이란 위탁자의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하는 방법을 말한다. 같은 법 시행령 제28조제3항에서는 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 어느 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하도록 규정하고 있다; ①위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법, ②관보(위탁자자 공공기관인 경우만 해당한다)나 위탁자의 사업자등이 있는 시·도 이상의 지역을 주된 보급 지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호 가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법, ③같은 제목으로 연2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법, ④재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

나. 「개인정보 보호법」 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)’, ‘개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)’등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 ‘고시’라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 하고, 비밀번호의 경우에는 복호화 되지 않도록 일방향 (해쉬함수)암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다. (제7조제2항)
- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지정보, 처리한 정보주체 정보를 기록하고 접속기록을 최소 1년 이상 보관·관리하여야 한다. 다만 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제처리하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부관리계획에 보관 기간을 정하고 이를 이행하여야 하며, 비인가자의 개인정보처리시스템에 대한 접속시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상행위 등에 대한 안전조치를 강화할 수 있도록 해야 한다. (제8조제1항)

2. 위법성 판단

가. 개인정보 처리 업무를 위탁하면서 수탁자 공개를 소홀히 한 행위 (법 제26조제2항)

피심인이 개인정보 처리 업무를 위탁하면서 일부 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하지 않은 사실은 「개인정보 보호법」 제26조제2항을 위반한 것이다.

나. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않은 사실(고시 제7조제2항), ②개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리한 사실(고시 제8조제1항)은 「개인정보 보호법」 제29조를 위반한 것이다.

< 피심인(성동구청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보처리 위탁시 (공개)	§26②	§28②	개인정보 처리 업무를 위탁하는 개인정보처리자는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 하나, 일부를 공개하지 않음
안전조치의무	§29	§30①	① 비밀번호를 저장하는 경우 일방향 암호화를 적용하지 않음 (고시 제7조제2항) ② 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 일부 항목이 누락된 접속기록을 보관·관리함 (고시 제8조제1항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 개인정보 처리 업무를 위탁하는 때에는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게

확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 한다.

나. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 비밀번호를 저장하는 경우 안전한 암호화 알고리즘으로 일방향 암호화 저장할 것

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 항목누락 없이 보관·관리할 것

다. 피심인은 가·나의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의 「개인정보 보호법」 제26조제2항, 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2021-002-038호
안 건 명	개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 의 인	계룡시청 충청남도 계룡시 장안로 46
의결연월일	2021. 1. 27.

주 문

1. 피심인 계룡시청에 대해 다음과 같이 시정조치를 권고한다.

가. 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 ①위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항, ②개인정보의 기술적·관리적 보호조치에 관한 사항, ③위탁업무의 목적 및 범위, ④재위탁금지에 관한 사항, ⑤개인정보에 대한 접근 제한 등 안전성 확보조치에 관한 사항, ⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항, ⑦수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상에 관한 사항이 모두 포함된 문서로 하여야 한다.

나. 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

다. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고 3년간 보관 할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

라. 가·나·다의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로 「지방자치법」 제2조에 따른 지방자치단체이다.

Ⅱ. 사실조사 결과

1. 조사 대상

개인정보보호위원회[30]는 「개인정보 보호법」 위반 여부에 대한 피심인의 개인정보 관리실태 현장 검사('20. 6. 29.~7. 2.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 처리 업무를 위탁하면서 위탁 목적 등을 문서화하지 않은 행위

피심인이 개인정보의 처리 업무를 수탁자에게 위탁하면서 「개인정보 보호법」에서 요구하는 내용을 모두 포함한 문서로 하여야 하나 이를 이행하지 않은 사실이 있다.

나. 개인정보 처리 업무를 위탁하면서 수탁자 관리·감독을 소홀히 한 행위

피심인은 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 하나, 이를 이행하지 않은 사실이 있다.

다. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 개인정보취급자의 접근권한 부여·변경·말소와 관련된 기록 중 일부

30) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라 개인정보보호위원회가 행정안전부 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제2항), 법 시행 전 행정안전부가 행한 고시·행정처분 중 그 소관이 행정안전부에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제3항)

를 보관하고 있지 않은 사실이 있다.

2) 피심인은 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유되는 사실이 있다.

3) 피심인은 개인정보취급자의 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

라. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 1.13.~2021. 1.25. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2021.1.22. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」제26조제1항 및 같은 법 시행령 제28조제1항에 따라 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음의 내용이 포함된 문서에 의하여야 한다; ①위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항, ②개인정보의 기술적·관리적 보호조치에 관한 사항, ③위탁업무의 목적 및 범위, ④재위탁 제한에 관한 사항, ⑤개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항, ⑥위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항, ⑦수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

나.「개인정보 보호법」제26조제4항은 "위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록

수탁자를 교육하고, 처리현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다"고 규정하고 있다.

1) '개인정보보호 법령 및 지침·고시 해설'(행정안전부, 2016.12)에 따르면 위탁자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. 또한, 위탁자는 수탁자가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위수탁 계약(법 제26조제1항 각호에 따른 사항)의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다. 따라서 위탁자는 수탁자에 대하여 정기적인 교육을 실시하는 외에 수탁자의 개인정보 처리현황 및 실태 목적외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사· 점검하여야 한다.

다. 「개인정보 보호법」 제29조는 "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다"고 규정하고 있다.

1) 「개인정보 보호법 시행령」 제30조제1항은 '개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)', '개인정보침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)'등을 하여야 한다고 규정하고 있다.

2) 「개인정보 보호법 시행령」 제30조제4항에 따라 기술적·관리적 및 물리적 조치의 기준 수립 및 시행에 관한 내용을 구체적으로 정하고 있는 「(舊)개인정보의 안전성확보 조치 기준」(행안부 고시 제2019-47호, 이하 '고시'라 한다) 및 동 고시 해설서에서는 다음과 같이 규정하고 있다.

- 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 이를 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 다수의 개인정보취급자가 동일한 업무를 수행한다고 하더라도 하나의 사용자계정을 공유하지 않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임추적성(Accountability)을 확보하여야 한다. (제5조제4항)
- 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드, 삭제·출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있으며, 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보처리시스템을 통합하여 점검할 수 있다. 특히 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다. (제8조제2항)

2. 위법성 판단

가. 개인정보 처리 업무를 위탁하면서 위탁 목적 등을 문서화 하지 않은 행위 (법 제26조제1항)

피심인이 개인정보 처리 업무를 위탁하면서 위탁 목적 등을 문서화 하지 않은 것은「개인정보 보호법」제26조제1항을 위반한 것이다.

나. 개인정보 처리 업무를 위탁하면서 수탁자에 대한 관리·감독을 소홀히 한 행위 (법 제26조제4항)

피심인이 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 안전하게 처리하는지를 감독하지 않은 사실은「개인정보 보호법」제26조제4항을 위반한 것이다.

다. 개인정보에 대한 안전조치 의무를 소홀히 한 행위 (법 제29조)

피심인이 ①개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록·보관하지 않은 사실(고시 제5조제3항), ②개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유한 사실(고시 제5조제4항), ③개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실(고시 제8조제2항)은「개인정보 보호법」제29조를 위반한 것이다.

< 피심인(계룡시청)의 위반사항 >

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
개인정보처리 위탁시 (문서)	§26①	-	업무위탁 시 위탁목적 등 법에서 요구하는 필수사항을 문서화하지 않음
수탁자 관리·감독	§26④		업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 하나, 이를 이행하지 않음

위반 내용	법령 근거		
	법률	시행령	세부내용(고시 등)
안전조치의무	§29	§30①	① 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하고 있지 않음 (고시 제5조제3항) ② 개인정보취급자 별로 사용자계정을 발급하지 않아, 사용자계정이 다른 개인정보취급자와 공유됨 (고시 제5조제4항) ③ 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않음 (고시 제8조제2항)

Ⅳ. 처분 및 결정

1. 시정조치 권고

가. 피심인은 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 ①위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항, ②개인정보의 기술적·관리적 보호조치에 관한 사항, ③위탁업무의 목적 및 범위, ④재위탁금지에 관한 사항, ⑤개인정보에 대한 접근 제한 등 안전성 확보조치에 관한 사항, ⑥위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항, ⑦수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상에 관한 사항이 모두 포함된 문서로 하여야 한다.

나. 피심인은 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자의 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

다. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 및 물리적 보호조치를 하여야 한다.

1) 개인정보처리시스템의 접근권한 등록, 변경, 말소에 대한 내역을 기록하고

3년간 보관할 것

2) 개인정보처리시스템에 접속할 수 있는 사용자계정 발급 시 개인정보취급자별로 사용자계정을 발급하고, 다른 개인정보취급자와 공유되지 않도록 할 것

3) 개인정보처리시스템의 접속기록을 월 1회 이상 점검할 것

라. 피심인은 가·나·다의 시정조치 권고에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

2. 징계권고

피심인이 "「개인정보 보호법」 위반에 따른 행정처분 통지"를 받은 이후에 안전하고 체계적인 개인정보 관리를 위한 개인정보 보호에 대한 조치를 소홀히 하여 3년 내 같은 「개인정보 보호법」 제29조(안전성 확보조치 의무)를 위반한 책임은 피심인의 대표자 및 개인정보 보호책임자 등에게 있다.

피심인에 대하여 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유로 「개인정보 보호법」 제65조제2항에 따라 대표자 및 책임 있는 임원을 포함한 책임자에 대하여 징계할 것을 권고한다. 그 결과를 처분통지를 받은 날로부터 30일 이내에 개인정보보호위원회에 통보하여야 한다. 다만 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 개인정보보호위원회로 통보하여야 한다.

Ⅴ. 결론

피심인의「개인정보 보호법」제26조제1항, 제26조제4항, 제29조 위반행위에 대하여 같은 법 제64조(시정조치 등) 제4항에 따라 최근 3년 내 같은 위반행위로 행정처분 등을 받은 사유에 대해서는 같은 법 제65조(고발 및 징계권고) 제2항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치권고에 불복이 있는 경우,「행정심판법」제27조 및「행정소송법」제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

2021년 1월 27일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　백 대 용　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　염 흥 열　(서 명)

위　　원　　이 희 정　(서 명)