http://kostat.go.kr

행정자료를 이용한
국가통계 작성 표준편람(II)

– 개인정보 보호편 –

2014. 9.

통계청 STATISTICS KOREA

조사관리국
행정통계과

Contents

작 성 취 지

통계청은 불응률 증가 등 열악한 조사환경을 극복하고 수요자 요구에 맞는 정책맞춤형 통계 작성, **국민의 응답부담 경감 및 저비용·고효율의 국가통계 생산시스템 구축**을 위해 2007년 통계법 전부개정을 통해 법적근거를 마련한 후 행정자료 이용을 확대하여 왔다.

통계작성 목적으로 행정자료를 보다 체계적 · 효율적으로 이용하기 위해 2011년 2월 「행정자료 활용 및 개인정보 보호 표준편람」을 제작 · 발간하였으나, 행정자료 이용 실무경험과 노하우 등의 축적이나 방법론 개발 부족 등의 사유로 구체적 · 실무적인 내용보다 다소 이론적인 내용이 많이 반영되었던 측면이 있었다.

최근 몇 년 동안 행정자료를 이용하여 「임금근로일자리행정통계」, 「귀농 · 귀촌인 통계」, 「개인별주택소유통계」 등 5종의 행정통계를 신규 개발하였고, 기존 조사통계 31종에 대한 항목대체나 검증보완 등에 행정자료를 많이 활용하게 됨에 따라 실무방법론이 많이 발전하였고, **정부3.0정책을 추진함에 따라 이를 뒷받침할 수 있도록 구체적인 행정자료 이용 실무방법**을 동 편람에 반영할 필요성이 생겼다.

또한, 최근 카드사 및 통신사 등의 **개인정보 유출** 사고로 개인정보의 불법 유통에 대한 경각심이 급증하였고, 이에 따른 개인정보보호 및 **보안강화 요구가 증대하는 등** 새로운 환경변화에 적극 대응할 필요가 있었다.

따라서 이번에 개정한 표준편람은 행정자료 이용편(Ⅰ)과 개인정보 보호편(Ⅱ)으로 나누어 발간하였다.

1 행정자료를 이용한 통계 개발 · 개선 · 대체 등 실제 사례, 외국의 행정통계 품질지표 및 시사점, **행정자료 이용 시 실제 적용할 수 있도록 통계 작성 단계별로 행정자료 이용방법 구체화**와 관련된 내용과

2 최근 개인정보 보호방안 내용과 행정자료를 이용한 통계 작성 시 요구되는 **세부적인 개인정보 보호절차와 관련된 내용을 주로 반영하였다.**

PART

I

행정자료를 이용한 국가통계 작성 표준편람(II)

개 요

PART I

개 요

1. 행정자료란?

○ 공공기관이 직무상 작성 · 취득하여 관리하고 있는 문서 · 대장 및 도면과 데이터베이스 등 전산자료를 말하며 통계자료는 제외(통계법 제3조)

* 예시 : 안행부의 주민등록자료, 국토부의 건축물대장, 국세청의 사업자등록자료 등

※ (법률상 유사용어) **공공데이터**란 데이터베이스, 전자화된 파일 등 공공기관이 법령 등에서 정하는 목적을 위하여 생성 또는 취득하여 관리하고 있는 광(光) 또는 전자적 방식으로 처리된 자료 또는 정보(공공데이터의 제공 및 이용 활성화에 관한 법 제2조)

* 예시 : 버스운행정보DB, 기상관측 DB, 각 분야의 연구보고서, 연도별 백서 · 통계연보 등

■ 통계자료 : 통계작성기관이 통계의 작성을 위하여 수집 · 취득 또는 사용한 자료(데이터베이스 등 전산자료를 포함)

* 예시 : 인구 · 주택총조사 자료 등

■ 공공 빅데이터 : 통계자료 및 행정자료 중 빅데이터 성격을 갖춘 자료

* 빅데이터 = 공공 빅데이터 + 민간 빅데이터(SNS, 인터넷정보 등)

2. 행정자료를 이용한 통계 생산의 필요성

○ 1·2인 **가구** 및 **맞벌이**가구, **외부인 출입통제** 주택 증가, 고령화, 등 **인구·가구·주택구조의 변화로 조사원의 응답자 접근성 약화**

* 1인 가구 비율(%)	:	('95)12.7	→	('00)15.5	→	('05)20.0	→ ('10)23.9
* 맞벌이가구 비율(%)	:	('03)25.9	→	('07)33.2	→	('09)35.6	→ ('11)43.6
* 공동주택 비율(%)	:	('95)49.2	→	('00)59.3	→	('05)66.5	→ ('10)71.6
* 65세이상 인구비율(%)	:	('95) 5.9	→	('00) 7.3	→	('05) 9.3	→ ('10)11.3

○ 개방, 공유, 소통, 협업을 핵심으로 하는 정부3.0의 성공적 구현을 위해 부처 간 협업을 통한 행정자료의 효율적 활용 요구 증대

○ (국내 추세) '공공데이터의 제공 및 이용 활성화에 관한 법률' 제정으로 공공기관이 보유·관리하는 공공데이터에 대한 국민의 이용권을 보장

○ 최근 통계청은 행정자료를 이용하여 정부정책의 수립 평가 등에 필요한 5종의 행정통계*를 신규 개발('13년말 기준)

* '임금근로일자리행정통계('12년)', '귀농·귀촌인통계('12년)', '기업생멸행정통계('12년)', '개인별주택소유통계('13년)', '영리법인기업체통계('13년)'

○ (국제적 추세) 미국, 유럽 등 선진국에서는 통계목적의 행정자료 이용이 점점 확대

– UN[1)2)], EU[3)] 등에서도 응답부담 경감, 비용절감 등을 고려하여 행정자료 이용을 적극 권장

---

1) **UN 공식통계 10대 기본원칙** (제5원칙 : 비용-효율성의 원칙)
통계목적으로 사용되는 자료는 통계조사나 행정자료 등 모든 형태의 자료출처로부터 수집될 수 있으며 이때 통계기관은 통계품질, 시의성, 비용 및 응답자 부담을 고려하여 수집 방법을 선택해야 한다(Diverse sources : Data for statistical purposes may be drawn from all types of sources, be they statistical surveys or administrative records. statistical agencies are to choose the source with regard to quality, timeliness, costs and the burden on respondents)

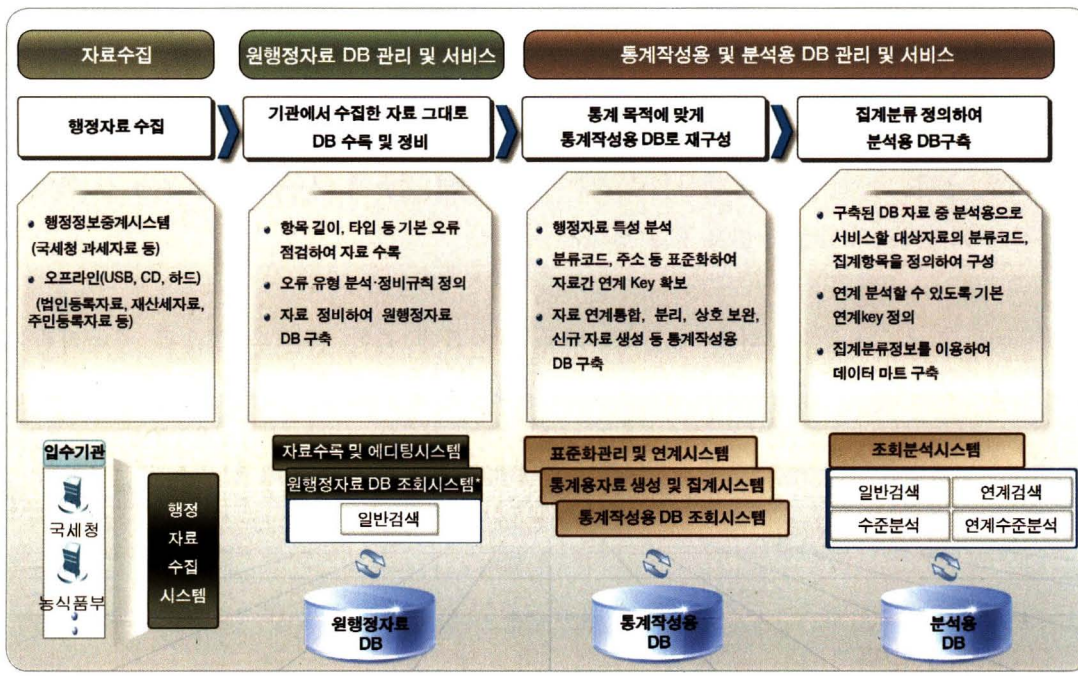
2) **UN에서는 2011년에 「공식통계를 위한 행정자료 이용 핸드북」** : (Using Administrative and Secondary Source for Official Statistics: A Handbook of Principles and Practices)을 제작하여 배포

3) **유럽통계청(Eurostat)의 '행정자료(administrative source)'란** : 통계를 주목적으로 수집된 자료뿐만 아니라 다양한 정보를 포함하는 자료원천을 말함[Business registers : Recommendations manual (2010 edition)]

3. 통계작성을 위한 행정자료 처리절차

○ 통계청에서는 2009년부터 행정자료를 수집하여 통계작성을 위하여 자료의 특성을 분석하여 표준화작업을 통하여 자료를 연계할 수 있도록 DB로 구축 · 관리

〈 원행정자료 DB 〉



4. 정보보호관리체계 구축

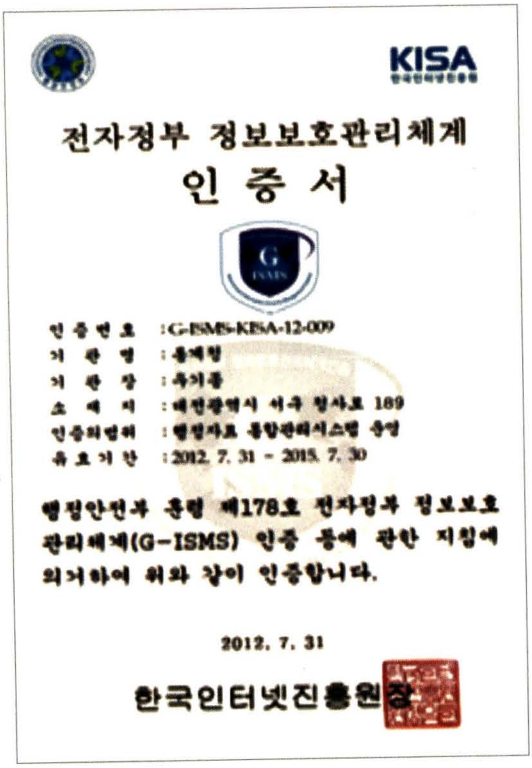
○ 통계청에서는 행정자료의 보호를 보다 강화하기 위하여 전자정부 정보보호관리체계(G-ISMS)의 인증을 취득함

※ G-ISMS(Government Information Security Management System)
– 기관이 수립하고 구축한 종합적인 정보보호관리체계를 제3자가 객관적으로 심사하여 인증을 부여하는 제도

- 인증기관: 한국인터넷진흥원
- 대상업무: 행정자료통합관리시스템, 사이버보안관제센터 운영

- 심사방법
  - · G-ISMS의 12개 분야 156개 통제항목 기준으로 우리청의 인증범위 대상에 대하여 현황파악 및 수준분석을 수행
  - · 정보보호 수준분석, 위험분석 및 평가, 정보시스템 취약점 분석 등
- 취득일자 : 2012. 7. 31. (유효기간 – 2015. 7.30, 3년)
- 인증유지조건
  - · 매년 1회 사후 심사를 거쳐 부적합 등 지적사항 보완 조치
  - · 유효기간(3년) 만료되는 당해 연도에 갱신 심사

〈 전자정부 정보보호관리체계 인증서 〉



KISA

전자정부 정보보호관리체계

인 증 서

인 증 번 호 : G-ISMS-KISA-12-009
기 관 명 : 통계청
기 관 장 : 우기종
소 재 지 : 대전광역시 서구 청사로 189
인증의범위 : 행정자료 통합관리시스템 운영
유 효 기 간 : 2012. 7. 31 - 2015. 7. 30

행정안전부 훈령 제178호 전자정부 정보보호 관리체계(G-ISMS) 인증 등에 관한 지침에 의거하여 위와 같이 인증합니다.

2012. 7. 31

한국인터넷진흥원장

KISA

전자정부 정보보호관리체계

인 증 서

인 증 번 호 : G-ISMS-KISA-12-010
기 관 명 : 통계청
기 관 장 : 우기종
소 재 지 : 대전광역시 서구 청사로 189
인증의범위 : 사이버보안관제센터 운영
유 효 기 간 : 2012. 7. 31 - 2015. 7. 30

행정안전부 훈령 제178호 전자정부 정보보호 관리체계(G-ISMS) 인증 등에 관한 지침에 의거하여 위와 같이 인증합니다.

2012. 7. 31

한국인터넷진흥원장

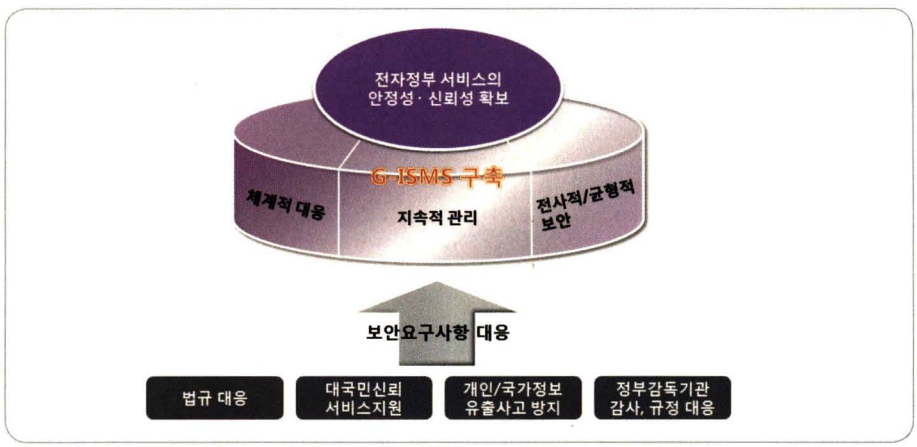
〈 전자정부 정보보호관리체계 인증서 〉

○ 전자정부 정보보호관리체계(G-ISMS) 인증은 기관이 수립하고 구축한 종합적인 정보보호 관리체계(ISMS)를 제3자가 객관적으로 심사하여 인증을 부여하는 제도

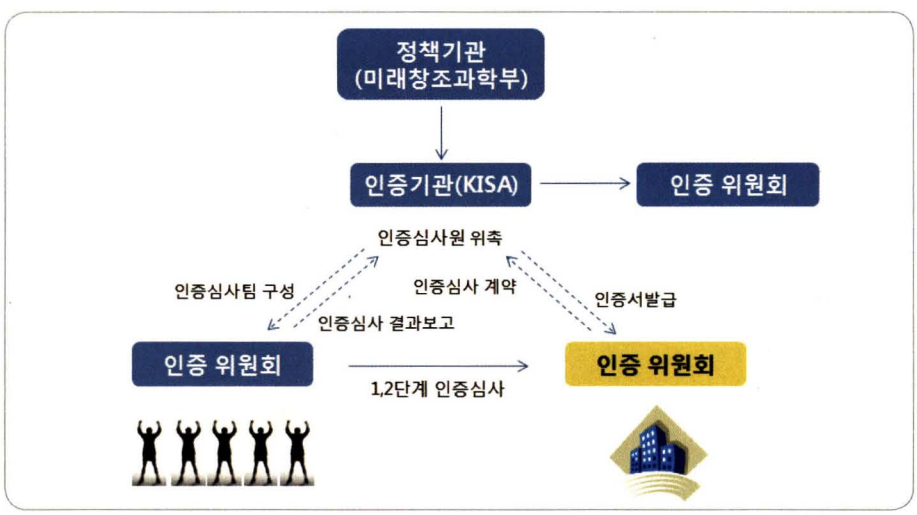
※ G-ISMS: Government Information Security Management System

○ 정보보호관리체계(ISMS)는 조직의 정보 자산을 체계적으로 보호하고, 사이버침해 위협으로부터 조직이 유기적으로 대응하기 위한 종합적인 관리체계

○ 전자정부 정보보호관리체계(G-ISMS)는 정부 행정기관 등의 조직 및 서비스의 특성에 적합하게 수립된 종합적인 정보보호 관리체계를 의미



○ G-ISMS 인증체계는 역할과 책임에 따라 정책기관, 인증위원회, 인증기관, 신청기관으로 구분합니다. 정책기관과 인증위원회는 미래창조과학부가, 인증기관은 KISA가 그 역할을 수행



PART

Ⅱ

행정자료를 이용한 국가통계 작성 표준편람(II)

국가통계 작성에 따른 개인정보보호 관련 규정

PART II

국가통계 작성에 따른 개인정보보호 관련 규정

1. 개인정보 보호 관련 법령

○ **(통계법)** 제4조의③(국가 등의 책무), 제24조(행정자료의 제공), 제24조의2(사법기관 등의 자료 제공), 제33조(비밀의 보호) 및 제34조(통계종사자 등의 의무)에 의하여 개인이나 단체 등의 비밀에 속하는 사항에 대한 비밀 보호 의무를 지고, 위반 시 제39조(벌칙), 제41조(과태료) 등에 의하여 처벌 규정

제4조의③ (국가 등의 책무) 통계작성기관의 장은 통계의 작성을 위하여 질문을 받거나 자료제출 등의 요청을 받고 답변을 하거나 자료제출 등을 하는 **개인이나 법인 또는 단체** 등(이하 "통계응답자"라 한다)의 부담을 최소화하고, **비밀이 보호되도록 노력하여야 한다.**

제24조(행정자료의 제공) ① 중앙행정기관의 장 또는 지방자치단체의 장은 통계의 작성을 위하여 필요한 경우에는 공공기관의 장에게 행정자료의 제공을 요청할 수 있다. 〈개정 2012.12.18〉

제24조의2(사법기관 등의 자료 제공) ① 통계청장은 통계의 작성을 위하여 필요한 경우에는 가족관계등록전산자료의 제공을 법원행정처장에게 요청할 수 있다.

[본조신설 2014.5.14.]

제33조(비밀의 보호) ① 통계의 작성과정에서 알려진 사항으로서 **개인이나 법인 또는 단체 등의 비밀에 속하는 사항은 보호**되어야 한다. ② 통계의 작성을 위하여 수집된 **개인이나 법인 또는 단체 등의 비밀에 속하는 자료는 통계작성 외의 목적으로 사용되어서는 아니 된다.**

제34조(통계종사자 등의 의무) 통계종사자, 통계종사자이었던 자 또는 통계작성기관으로부터 통계 작성업무의 전부 또는 일부를 위탁받아 그 업무에 종사하거나 종사하였던 자는 **직무상 알게 된 사항을 업무 외의 목적으로 사용하거나 다른 자에게 제공하여서는 아니 된다.**

제39조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

제41조(과태료) ③ 다음 각 호의 어느 하나에 해당하는 자에게는 100만원 이하의 과태료를 부과한다.

○ **(개인정보 보호법)** 제1장(총칙) ~ 제9장(벌칙)에 개인정보 보호 원칙, 국가 등의 책무, 개인정보 보호지침, 벌칙 등이 규정되어있음. 동 법 제58조(적용의 일부 제외)에 공공기관이 처리하는 개인정보 중 **「통계법」에 따라 수집되는 개인정보에 대해서는 제3장부터 제7장까지 적용 제외***됨.

* 제3장 개인정보의 처리, 제4장 개인정보의 안전한 관리, 제5장 정보주체의 권리 보장, 제6장 개인정보 분쟁조정위원회, 제7장 개인정보 단체소송

2. 내부규정

○ **(내부운영 규정)** 내부적으로 「행정자료의 정보보호에 관한 규정」 및 「정보보안업무 규정 시행세칙」을 제정하여 정보보안을 강화

- **(행정자료의 정보보호에 관한 규정)** 통계법 제24조에 따른 **행정자료의 접수, 보관 및 활용에 있어서 개인이나 법인 또는 단체 등의 정보를 보호**

  · 행정자료의 접수부터 관리, 자료처리까지 각 단계별 보안 사항 규정

- **(정보보안업무 규정 시행세칙)** 국가 정보보안 기본지침, 국가 사이버안전 매뉴얼, 개인정보 보호법에 따라서 정보보안활동에 필요한 세부사항을 규정

  · 통계청 전체의 개인정보보호 업무 총괄책임자(CPO)는 통계정보국장이 담당하고 정보시스템 접근 시 반드시 사용자 인증과정을 거쳐야 접근이 가능

가. 「행정자료의 정보보호에 관한 규정」(예규 제70호 2011. 7.22, 일부발췌)

- **제1조(목적)** 통계법에 따른 **행정자료의 접수, 보관 및 활용에 있어서 개인이나 법인 또는 단체 등의 정보를 보호**
- **제5조(자료접수)** 행정자료 입수 시 온라인을 통한 자료접수 원칙, 오프라인 시 보안적합성 검증을 필한 USB 메모리 등으로 제한
- **제7조(자료관리)** DB를 구축하여 자료를 보관 · 활용하는 경우 자료의 등록부터 폐기까지의 모든 이력을 DB에서 관리. 자료제공기관이 자료의 열람을 요구 시 공개 의무
- **제9조(자료처리)** ① 자료접근권자는 지정된 PC를 통해서만 인가된 자료에 대하여 비교 · 분석 · 생성 등 자료처리를 할 수 있으며, 행정전자 서명으로 본인임을 확인하여야 함. ③ 자료처리과정에서 개체식별자료를 다운로드 또는 저장("화면캡쳐" 포함)할 수 없도록 프로그램을 설치 · 운영
  ④ 자료에 대한 활용이 종료 시 자료의 활용과정에서 생성된 개체식별정보가 기록된 인쇄물 및 전자파일 등 생성자료를 복구할 수 없는 방법으로 폐기

나. 「정보보안업무 규정 시행세칙」(훈령 제251호 2012. 3.30. 일부발췌)

- **제1조(목적)** 국가 정보보안 기본지침, 국가 사이버안전 매뉴얼, 개인정보보호법에 따라서 통계청 정보보안활동에 필요한 세부사항 규정
- **제14조(개인정보보호 관리체계)** 통계청 전체의 개인정보보호 업무 총괄책임자(CPO)는 통계정보국장이 담당, 영상정보관리자는 운영지원과장이 담당
- **제21조(접근 통제)** ① 통계청의 모든 정보시스템은 반드시 사용자 인증과정을 거쳐야 접근이 가능하도록 함. ② 정보보안담당관은 각 정보시스템의 사용자가 관리자 권한으로 접근하고자 할 경우 IP 주소를 이용하여 특정 단말에서만 접근이 허용하도록 조치하여야 한다. ③ 시스템 관리자는 동일한 계정으로 여러 명이 동시에 정보시스템에 로그인하지 못하도록 차단하여야 하며, 업무상 필요한 경우에 정보보안담당관의 승인을 받아 제한적으로 그룹 계정을 사용할 수 있다.

※ "정보보안" 또는 "정보보호" 란 정보통신수단으로 수집 · 가공 · 저장 · 검색 · 송수신 되는 정보의 유출 · 위변조 · 훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적 · 물리적 · 기술적 수단을 마련하는 일체의 행위를 말한다.

다. 「통계청 개인정보보호지침」(통계청예규 제103호 2013.04.02. 일부발췌)

- **제1조(목적)** 이 개인정보 보호지침(이하 "지침"이라 한다)은 「개인정보 보호법」(이하 "법"이라 한다) 에 따라 개인정보보호에 필요한 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.
- **제3조(적용범위)** 이 지침은 전자적 처리 여부를 불문하고 수기문서를 포함한 모든 형태의 개인정보파일을 운용하는 통계청과 통계교육원, 통계개발원, 지방통계청(이하 '소속기관'이라 한다)의 직원 및 계약관계에 있는 외주 직원에게 적용된다.
- **제5조(다른 지침과의 관계)** 통계청이 보유한 개인정보 중 통계법에 따라 수집된 행정자료 및 통계조사자료에 관해서는 본 지침이 적용되지 않으며, 「행정자료의 정보보호에 관한 규정」 및 「정보보안업무규정시행세칙」이 적용된다.

PART

Ⅲ

행정자료를 이용한 국가통계 작성 표준편람(II)

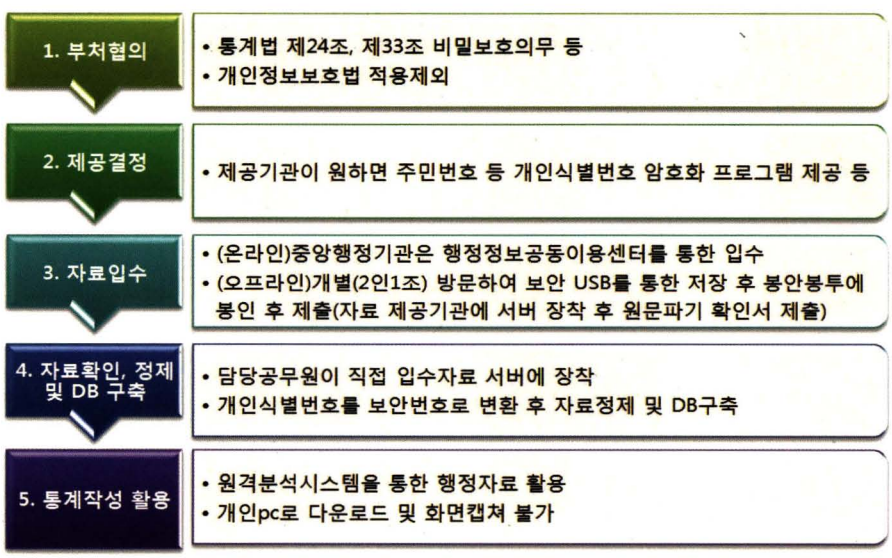
행정자료 입수 및 활용 단계별 개인정보보호

PART Ⅲ

행정자료 입수 및 활용 단계별 개인정보보호

■ 행정자료 활용시 단계별 개인정보보호 흐름도

○ 행정자료 보유 기관과 부처협의 단계부터 통계작성 활용 단계까지 개인정보보호 흐름도는 다음과 같다.



1. 부처협의 단계

○ 통계법에 의해 수집되는 개인정보는 개인정보보호법 제58조 제1항 제1호에 따라 제3장부터 제7장까지 **적용이 제외**되므로, **주민등록번호가 포함된 행정자료를 수집하는 경우 공공기관은 자료제공 요청에 응하여야함**

※ **「개인정보 보호법」과 「통계법」상의 개인정보 관계 질의 회신 내용**(2012. 1. 9, 행정안전부 개인정보보호과 회신)

1. 질의요약

통계법 제24조(행정자료의 제공)의 규정에 의거하여 통계청이 농림수산식품부에 주민등록번호 등 개인정보가 포함된 행정자료(홍성군 농업경영체 등록자료)를 요청하여 수집하는 경우에도 개인정보보호법 제24조(고유식별정보의 처리 제한)가 적용되는지 여부

2. 답변내용

통계법에 따라 수집되는 개인정보는 개인정보보호법 제58조 제1항 제1호에 따라 제3장부터 제7장(같은 법 제15조부터 제57조까지를 말함)까지 적용이 제외되므로, 주민등록번호가 포함된 행정자료를 수집하는 경우에도 같은 법 제24조가 적용되지 않습니다.

- 또한, **통계법은 행정자료의 제공(제24조), 사법기관 등의 자료제공(제24조의2), 비밀보호 의무(제33조)와 위반할** 경우 **벌금(제39조), 과태료(제41조) 등 처벌을 규정**하여 행정자료의 정보보호 의무를 명시

○ **개인정보의 외부유출을 차단하고 정보보호를 위하여** 일반망(인터넷)과 물리적으로 분리된 **업무전용망을 설치**하고, **원격서버분석시스템을 도입**하여 모든 업무는 사전 허가된 자가 원격서버에서만 작업을 할 수 있으며, 개인PC에 자료를 다운로드하는 것은 **원천적으로 불가능**

2. 제공 결정

■ **국가통계 작성 목적의 행정자료를 제공 요청 받은 공공기관은 내부적으로 어디까지 제공할 것인지 여부 결정**

※ 행정자료 제공기관은 개인정보보호법 및 관련법에 따른 개인식별번호인 주민번호를 꼭 제공하여야 하는지 여부에 대해 검토

▶ 안행부의 재산세 자료는 지방세기본법을 개정(2014.1.1)하여 자료제공 결정. 농식품부의 농업경영체자료는 관련법에 개인식별번호는 제공하지 못하도록 규정 되어있으나 안행부의 유권해석에 따라 자료 제공

○ 주민등록번호 13자리는 1차적으로 통계보안번호 64자리로 변환되고 2차 8자리로 변환됨

○ 행정자료 보유기관은 통계청이 제공하는 1차 변환 프로그램을 사용하여 주민등록번호를 보안번호로 변환 후 제공 가능

- 향후 통계청은 현재 2차 변환에서 3차 변환을 통하여 주민등록번호 암호화 추진 예정

3. 자료입수(온라인, 오프라인)

○ **(온라인)** 중앙행정기관은 '행정정보공동이용센터'(중개 시스템 역할)를 통하여 제공 받는 것을 원칙으로 함

- 전송 후 동 센터에서 문서코드(6자리)를 찾아 통계청 서버로 다운로드
- 서버와 서버 간 자료제공으로 중간 해킹 등 방지할 수 있으며 가장 안전한 자료 입수 방법임

○ **(오프라인)** '행정정보공동이용센터'를 이용할 수 없는 공공기관은 통계청 직원(2인 1조)이 보안 USB 또는 CD를 사용하여 자료 입수

- (입수 및 파기 절차) 행정자료 제공 담당자에게 보안 USB(또는 CD)제출 → 자료다운로드 → 제공기관은 USB 및 CD를 봉투에 넣고 봉인 후 인계인수서 작성 → 통계청 정보화기획과 제출 → 담당공무원이 봉인 확인 후 직접 서버에 장착 → USB(또는 CD)에 저장된 원자료 파기(정보화기획과) → 제공기관에 공문으로 확인서 제출

4. 자료 확인, 정제 및 DB구축

○ 공공기관으로부터 제공받은 행정자료는 담당 공무원이 직접 서버에 장착 후 관리적, 물리적, 기술적 보안이 구비된 별도의 공간에서 외주 용역업체가 레이아웃, 자료형태 확인, 주민번호의 보안번호*로 변환 및 자료정제 후 행정자료DB시스템에 업로드

* 주민등록번호는 1차 변환 64자리, 2차 및 3차 8자리 보안번호로 변환

〈 외부 용역사업 관련 보안조치 사항 〉

- 외부 용역사업 추진 시 계약서*에 **참여직원의 보안준수 사항과 위반 시 손해배상 책임** 등을 명시
- 사업 완료 후 생산되는 최종 산출물에 대해 **복사본 등 용역사업 관련 자료를 보유하지 않는다는 내용이 포함된 대표명의 확약서를 징구**
- 용역업체에 제공할 자료는 보안조치 후 인계인수대장에 이를 작성하고 **무단복사 · 외부반출을 금지**
- 용역 참여직원이 노트북 등 관련 장비를 **반출 또는 반입할 때마다 정보보안담당관의 승인**을 받아야 하며, **정보보안담당관은 악성코드 감염여부, 자료 무단반출 여부를 확인**
- **용역사업 종료 시 외부업체의 노트북 · 보조기억매체 등을 통해 기관 내부자료 및 용역 결과물이 유출되는 것을 방지**하기 위하여 **복구가 불가능하도록 완전소거** 하는 등 보안조치
- 시스템 관리자는 필요한 경우를 제외하고는 **외부 인력의 정보시스템 접근권한을 차단**
- 상주 용역 인원은 업무개발실 등 **독립적인 공간에서 근무**하여야 하며 **비인가자의 출입 및 접근은 기술적으로 통제하고 지문인식장치** 등을 활용한 **비인가자의 출입 및 접근을 통제**

※ 상기에 언급되지 않은 내용은 국가정보원 「국가 · 공공기관 용역업체 보안관리 가이드라인」 (2014.3.) 준수

5. 통계작성 활용

○ 통계작성에 활용하기 위해서는 사전에 행정자료 이용 신청서를 작성하여 담당과에 제출하면 원격분석시스템에 접근할 권한이 주어짐

- 동 서버에서만 자료 분석이 가능하고 개인PC로의 다운로드 및 화면캡쳐는 불가

PART

Ⅳ

행정자료를 이용한 국가통계 작성 표준편람(Ⅱ)

행정자료 이용에 따른 개인정보 보호 체계

PART Ⅳ

행정자료 이용에 따른 개인정보 보호 체계

○ **(행정자료 이용절차)** 행정자료를 이용하기 위해서는 자료이용신청서 제출, 자료접근권자 등재, 본인확인, 자료이용 후 생성된 개체식별번호 등 폐기 절차를 준수

〈 원격분석시스템 구성도 〉

자료관리 책임자에게 자료이용신청서 제출(서약서 포함)

↓

자료접근권자 관리대장(정기, 수시)에 등재

↓

전자서명에 의한 본인확인

↓

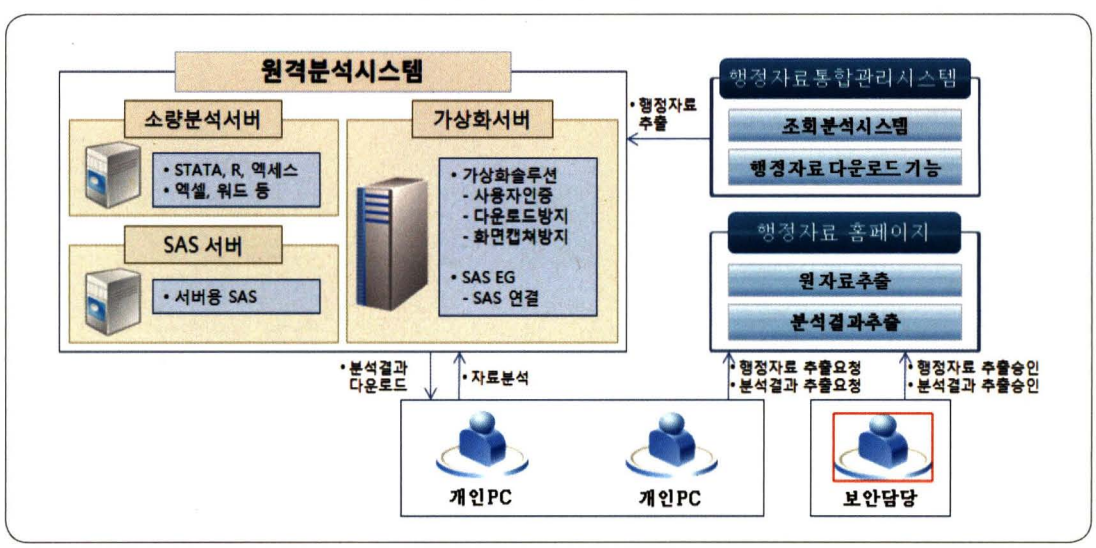
자료활용 종료 시 생성된 개체식별번호 등 폐기

〈 행정자료 접속기록의 관리 및 보관 〉

○ 행정자료 이용자가 자료처리 내역을 자동으로 기록할 수 있도록 관련 프로그램을 PC에 설치

- 자료접근권자의 성명/소속/직급, 활용한 행정자료명, 작업내용, 접속시간 등 체크

〈 원격분석시스템 구성도 〉



〈 원격분석시스템 이용절차 〉

절차	방법	담당과
사용자 등록신청	[행정자료 홈페이지] · 원격분석시스템 사용자등록 요청	사용자
사용자 등록	[방화벽 설정 요청] · 정보화기획과에서 통합센터로 방화벽 설정요청	정보화기획과
	[사용자 계정 등록] · 원격분석시스템 및 서버용SAS 사용자 등록	조사시스템 관리과
SAS 프로파일 등록	[원격분석시스템] · 원격분석시스템을 통하여 서버용SAS에 접속 · SAS 프로파일 등록	사용자
행정자료추출요청	[행정자료 추출요청] · 행정자료 홈페이지에서 원격분석결과요청	사용자
	[행정자료 추출 승인] · 행정자료 홈페이지에서 원격분석결과 추출 승인	정보화기획과
	[행정자료 추출] · 유지보수팀에서 추출하여 원격분석시스템에 탑재	행정자료 유지보수팀
원격분석	· 원격분석시스템을 이용한 원격분석	사용자
분석결과추출	[분석결과 추출요청] · 행정자료 홈페이지에서 원격분석결과요청	사용자
	[분석결과 추출 승인] · 행정자료 홈페이지에서 원격분석결과 추출 승인	정보화기획과
	[분석결과 추출] · 행정자료 홈페이지에서 분석결과 다운로드	사용자

1. 행정자료 이용에 따른 개인정보 보호 체계

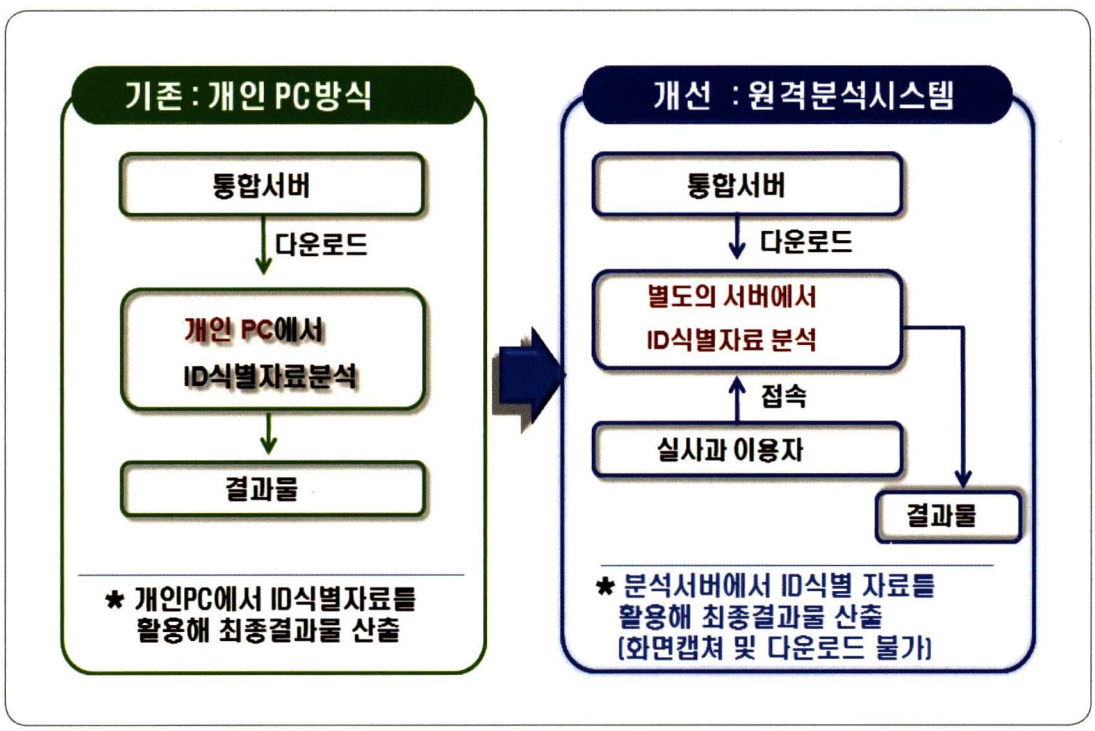
1 행정자료 보안을 위해 인터넷망과 분리된 폐쇄망 구축

○ **(보안 기술이 적용된 시스템 구축)** 입수된 행정자료는 보안기술이 적용된 행정자료데이터베이스로 구축하여 **행정자료 통합관리시스템으로 집중 관리**

○ **(내 · 외부망 분리)** 외부 인터넷망을 통해 내부망에 침투하여 개인 컴퓨터 및 DB자료의 해킹 방지 및 네트워크에 대한 보안 강화를 위해 **내 · 외부망 분리**

- **인가된 저장 매체(보안 USB)만을 업무망 및 인터넷망에 접속**가능 하도록 통제

○ **('원격분석시스템' 구축)** 행정자료를 개인PC가 아닌 별도의 서버에서만 분석하도록 하여 개인정보 유출을 방지('12.1월 서비스)



※ 참고로 마이크로데이터는 개인을 식별할 수 없도록 처리(Masking 기법)하여 제공하고 있음

2 행정자료에 대한 접근 통제

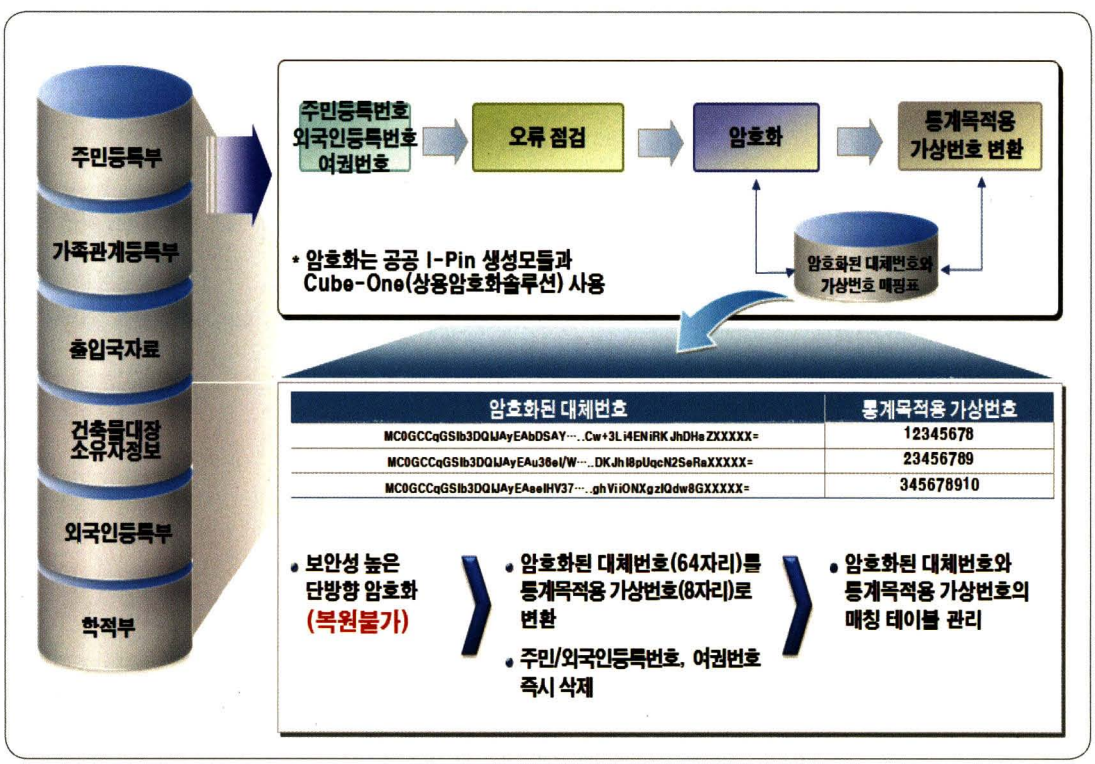
○ (행정자료 통합관리시스템 접근 제한) 행정자료 통합관리시스템은 공인인증서 로그인방식, 로그인 실패횟수 3회 제한, 시스템 장시간 미사용 시 자동 로그아웃 등 기술적 보안조치

- 또한, 보안관리자가 접근권한을 부여하고 모든 접근 기록을 관리

○ (암호화된 보안 식별번호 사용) 입수한 행정자료에 개인 식별번호(주민등록번호 등)는 암호화를 거쳐 보안식별번호로 대체

▶ 보안식별번호 대체 후 기존의 주민등록번호 등은 삭제하여 개인정보의 유출을 원천적으로 방지

〈 주민등록번호, 외국인등록번호, 여권번호는 암호화한 보안식별번호 사용 〉



○ (자료 전송구간 암호화 및 DB암호화) 로그인 및 회원정보 등 개인정보가 전송되는 구간의 암호화(SSL*) 및 개인정보가 저장되는 데이터베이스에 대한 암호화 의무

* SSL (Secure sockets layer) : 보안 소켓 계층을 이르는 말로, 인터넷에서 데이터를 안전하게 전송하기 위한 인터넷 통신 규약 프로토콜

3 통계청의 모든 통계자료는 **정부통합전산센터의 사이버안전센터 및 통계청 사이버 보안관제센터*를** 통하여 **실시간으로 감시**하고 있으며, **방화벽 이중화와 침입방지 시스템 등 보안장비 설치 운영**

* 사이버 보안관제 센터 : 국가정보원(국가사이버안전센터), 기획재정부(재정경제 사이버안전센터)와 연계하여 공동 대응체계유지

○ (보안관제 수행 절차) 국가정보원 국가사이버안전센터에서 사이버 위협이 증가되는 경우 사이버 위기경보를 발령

〈 침해 등급별 수행내용 〉

침해 등급	대응시간	내용
심각	즉시	악성코드 영향으로 인해 가용중인 서비스에 심각한 영향을 미칠 때
경계	30분 이내	위험요소의 증가함이 모니터링 되며, 웜바이러스의 확산속도가 빠를 시 대응
주의	2시간 이내	위험에 노출된 자원에 대한 면밀한 조사와 로그의 모니터링 수행. 웜바이러스 확산 위험 존재 시 대응.
관심	24시간 이내	위험요소의 발생 가능성이 의심되어 모니터링 수행, 위험도 낮은 웜바이러스 발생 시 대응.

4 기타, 개인정보 취급업무 관련 **외주용역 사업 시 조치사항**

○ DB구축 및 시스템 개발 등을 위해 외주용역사업자가 개인정보를 취급하는 경우 계약서에 다음 내용을 포함

- 용역업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 기술적 · 관리적 보호조치에 관한 사항
- 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
- 용역업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
- 의무를 위반한 경우의 손해배상 등 책임에 관한 사항 등

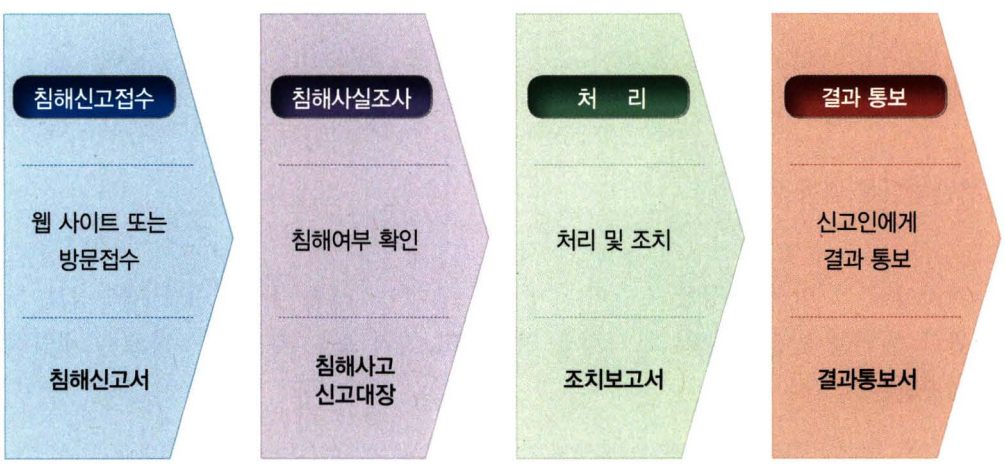
2. 개인정보 유출 통지 및 신고

○ 개인정보취급자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 통계청 개인정보관리책임관(CPO, 통계정보국장) 및 자료제공기관에 아래 각 호의 사실을 알려야 함

- 유출된 개인정보의 항목
- 유출된 시점과 그 경위
- 개인정보취급자의 대응조치 및 피해 구제절차
- 피해신고 등을 접수할 수 있는 담당부서 및 연락처

○ 유출된 개인정보의 규모가 1만 명 이상인 정보주체에 해당할 때에는 안전행정부장관 등에 대상 신고 및 홈페이지 공개(7일 이상) 병행

〈 개인정보 침해 시 신고 처리절차 〉



3. 법률상 개인정보 위반에 대한 처벌 규정

가. 통계법

○ 개인이나 법인 또는 단체 등의 비밀에 속하는 사항을 그 목적 외의 용도로 사용하거나 이를 다른 자에게 제공한 자

▶ 3년 이하의 징역 또는 1천만 원 이하의 벌금

○ 공공기관으로부터 제공받은 행정자료(비밀에 속하는 사항을 제외한다)를 제공받은 목적 외의 목적으로 사용하거나 다른 자에게 제공한 자

▶ 100만 원 이하의 과태료 부과

나. 개인정보보호법

○ 위반행위에 대한 처벌

- 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받은 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

▶ 3년 이하의 징역 또는 3천만 원 이하의 벌금

- 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 또는, 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위

▶ 5년 이하의 징역 또는 5천만 원 이하의 벌금

- 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 발송하여 공공기관의 업무 수행의 중단 · 마비 등 심각한 지장을 초래한 자

▶ 10년 이하의 징역 또는 1억 원 이하의 벌금

○ 개인정보 피해구제

- **손해배상책임** : 개인정보처리자의 고의 · 과실이 입증되면 개인정보처리자에게 손해배상책임을 청구
(개인정보보호법 제39조)

- **집단분쟁조정** : 권리침해가 다수의 정보주체에게 비슷한 유형으로 발생하는 경우 분쟁조정위원회에 일괄 조정 의뢰
(동법 제49조)

- **개인정보 단체소송** : 개인정보처리자가 집단분쟁조정 거부 시 법원에 권리침해 행위의 금지 · 중지를 구하는 소송
(동법 제51조)

PART V

행정자료를 이용한 국가통계 작성 표준편람(II)

외주인력 보안통제 조치

PART V 외주인력 보안통제 조치

○ **(현황)** 행정자료 입수 이후 DB구축 등 주로 외주 용역사업으로 이루어지는 상황에서 외주인력의 통제는 매우 중요함

○ **(문제점)** 최근 카드사태 등 외주 업체에서 개인정보 유출 등 보안사고가 잦으나 이에 대한 적절한 기술적 · 관리적 보안대책을 마련하지 않아 발생

○ **(대책)** 따라서 외주인력에 대해 필수적으로 준수해야할 기술적 · 관리적 보호대책을 제시

1. IT외주용역의 유형

○ IT 외주용역 유형은 **접근 IT자원**, 자원사용권한, 접근경로에 따라 5가지유형으로 분류

〈 IT 외주용역 유형 분류표 〉

IT 외부용역 유형		용역 특성				
		접근 IT 자원		자원 사용 권한		접근경로
유형1	운영 용역	내부 데이터	o	읽기	o	온라인
		IT 시스템	o	쓰기	o	
유형2	유지보수 용역	내부 데이터	o	읽기 (내부직원 동행)	x (o)	온라인
		IT 시스템	o	쓰기 (내부직원 동행)	x (o)	
유형3	SI 용역	내부 데이터	o	읽기	o	온라인
		IT 시스템	o	쓰기	x	
유형4	데이터 처리 용역	내부 데이터	o	읽기	o	온라인
		IT 시스템	x	쓰기	x	
유형5	오프라인 지원	내부 데이터	o	읽기	o	오프라인
		IT 시스템	x	쓰기	x	

2. 외주용역 단계별 보안강화 방안

○ 외주용역 추진 시 담당자 관점에서 단계별 정보보호 고려사항 및 대응지침을 제시함

가. 입찰 및 계약 단계

○ 용역 환경에 대한 사업계획서 작성단계에서부터 사전 보안 요구사항 도출 및 반영

정보보호 활동	세부 내용
1) 보안 요구 기준 마련	외주용역 추진에 있어서 제도, 정책, 지침 등에 따라 요구되는 정보보호 요구사항, 수준 등 기준을 마련하고 확인
2) 보안을 고려한 계약 체결	정보보호 요구사항이 반영된 사업자를 선정하고 미흡한 경우에는 기술협상 과정에서 정보보호 요구사항을 명확히 반영하여 계약 체결

1) 보안 요구 기준 마련

○ 외주용역과 관련된 정보 및 시스템에 대한 보안위험을 파악하고, 적절한 통제 방안을 구상

〈 외주용역 통제 기준 〉

- 외부자가 접근 가능한 정보의 식별 및 접근 형태의 분석
- 접근 가능한 정보의 중요 가치, 사업에 미치는 영향
- 비 인가된 정보에 대한 접근제한을 위한 통제 방안
- 인가된 외부자의 식별 방법 및 승인 사항의 재확인
- 필요한 외부자의 접근 요구가 불가능할 경우 미치는 영향
- 침해사고 및 잠재적인 손실 발생 시 외부자 접근 방안
- 외부자에게 제공하는 정보통신망 구성도, 세부 IP현황, 개인정보 등 중요정보 보안대책
- 용역 직원의 노트북 등 장비 반출 · 입에 대한 보안조치
- 업무과정에서 생산되는 산출물 및 최종 산출물 보안 관리
- 위탁서비스 운영 시 발생하는 보안사항의 위반 또는 침해사고 조치 방안

2) 보안을 고려한 계약 체결

○ 용역사업에 투입되는 자료 · 장비 등에 대한 대외보안이 필요한 경우 책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서와 개인정보보호관련 위탁계약서(별지 제8호 서식)를 작성

- 비밀유지계약서에는 비밀정보의 범위, 보안 준수사항, 위반 시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시

○ 용역사업 참여인원은 용역업체 임의로 교체할 수 없도록 명시하고 신상 변동사항 발생 시 발주업체에 즉시 보고

○ 발주업체의 요구사항을 사업자에게 명확히 하기 위해 과업지시서에 자료 보안관리 방법, 인원 · 장비 · 시설 등에 대한 보안점검 상세히 기술

○ 용역업체가 사업에 대한 하도급 계약을 체결할 경우 본 사업계약 수준의 비밀유지 조항을 포함토록 조치

○ 기관의 정보 또는 정보처리시설에 대하여 외주용역 직원의 접근을 허용할 경우 기관의 보안 요구사항을 계약서상에 명시

나. 개발 및 구축 단계

○ 내부 중요정보 유출 방지를 위한 기술적 조치와 외주인력의 정보유출 방지를 위한 인력관리 대책을 마련

정보보호 활동	세부 내용
1) 자료에 대한 보안 관리	내부자료 관리 계획을 수립하여 내부정보 유출 방지
2) 사무실 · 장비에 대한 보안관리	외주업체 사무실의 물리적 보안조치에 대해서 확인하고 외주 인력이 반 · 출입하는 장비에 대한 보안관리 계획을 수립하고 이행
3) 내 · 외부망 접근 관리	외주인력의 내부시스템 접근에 대한관리 및 외부망 접근제어
4) 외주인력 신원조회	외주인력을 통한 정보유출을 막기 위해 보안서약서 작성 및 사전 신원조사 실시

1) 자료에 대한 보안관리

○ 네트워크 구성도, IP현황, 개인정보 등 용역업체에 제공하는 비공개 자료는 별지 제9호 서식 (용역사업관리용) 자료제공대장을 작성하여 인계자(보안 책임자)와 인수자(용역업체 관리책임자)가 직접 서명한 후 인계 · 인수

○ 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 발주업체의 파일서버에 저장하거나 보안책임자가 지정한 PC에 저장 · 관리

○ 용역사업 관련 자료는 인터넷 웹하드 등 인터넷 자료 공유사이트 및 개인 메일함에 저장을 금지하고 전자우편을 이용해 자료전송이 필요한 경우 자체 전자우편을 이용, 첨부자료는 암호화 후 수 · 발신(단, 대외비 이상의 비밀은 전자우편으로 수 · 발신 금지)

○ 발주업체가 제공한 사무실에서 사업을 수행할 경우 제공한 비공개자료는 매일 퇴근 시 반납토록 하며 비밀문서를 제외한 일반문서는 용역업체에 제공된 사무실에 시건 장치가 된 보관함이 있을 경우 이에 보관 가능

○ 용역사업 수행으로 생산되는 산출물 및 기록은 용역관리담당자가 인가하지 않은 비인가자에게 제공 · 대여 · 열람을 금지

○ 정보시스템은 사용자별, 업무별 접근권한을 설정

○ 입 · 출력 및 수정사항, 관련자의 시스템 데이터 접근 내역 등에 대한 기록 관리

2) 사무실 · 장비에 대한 보안관리

○ 용역사업 수행 장소는 발주업체가 시건 장치와 통제가 가능한 공간을 제공하거나 협의를 통해 동일한 환경이 구축된 외부 사무실을 사용

○ 용역업체 사무실 또는 용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시

○ 발주업체 사무실에서 용역사업을 수행할 경우 용역 참여 직원이 노트북 등 관련 장비를 반출 또는 반입 시 악성코드 감염여부 및 자료 무단반출 여부를 확인

○ 인가받지 않은 USB 등의 휴대용저장매체 사용을 금지하며 산출물 저장을 위해 휴대용저장매체가 필요한 경우 보안 책임자의 관리 하에 사용

3) 내 · 외부망 접근 시 보안관리

○ 사업 참여인원에 대한 사용자 계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여

○ 계정별로 부여된 접속권한은 불필요 시 곧바로 권한을 해지하거나 계정을 폐기

○ 참여인원에게 부여한 패스워드는 사업관리부서에서 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인

○ 사업관리부서에서는 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근기록을 주기적으로 확인하여 이상 유무 확인

○ 사업 수행 상 필요한 경우에는 용역업체의 관리책임자가 직접 요청하고 보안책임자는 필요성이 인정될 경우 접속할 노트북을 지정하고 필요한 사이트에만 접속토록 방화벽 등 보안 조치 후 통제 후 사용

4) 외주인력 신원확인 및 보안 준수

○ 용역사업 참여인원에 대해서는 각 개인의 친필 서명이 들어간 보안서약서를 징구

○ 용역사업 수행 전 참여인원에 대해 신원을 확인하고, 법적 또는 발주업체 규정에 의한 비밀유지 의무 준수 및 위반 시 처벌내용 등에 대한 보안교육 실시

다. 사업완료 단계

○ 사업 완료 시 최종결과물 및 사업 중 사용된 장비, 자료의 외부 유출을 방지하기 위하여 자료의 수거 및 처리 방법에 대한 대책을 마련함

- 사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성 · 관리하고 불필요한 자료는 삭제 및 세단 후 폐기

- 용역업체에 제공한 제반자료, 장비, 서류와 중간 · 최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도 보관을 금지

- 노트북 · 보조기억매체 등 전자적으로 기록된 자료는 '정보시스템 저장매체불용처리 지침'에 따라 보안조치

〈정보시스템 저장매체불용처리 지침 〉

구분	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
광디스크	완전파괴 (소각. 파쇄. 용해)	완전파괴 (소각. 파쇄. 용해)	완전파괴 (소각. 파쇄. 용해)
자기 테이프	파괴 또는 삭제	파괴 또는 삭제	파괴 또는 완전포맷
반도체메모리 (EEPROM 등)	완전포맷 3회 수행	완전포맷 3회 수행	완전포맷 3회 수행
	완전포맷이 되지 않는 저장매체는 완전파괴		
하드디스크	완전포맷 1회 수행	파괴, 삭제, 포맷	파괴, 삭제

라. 유지보수 단계

○ 정보시스템 운영위탁 및 유지보수 단계에서 발생할 수 있는 시스템 불법 접근 등에 대한 대책마련과 접근방법에 대한 대책을 마련

○ 위탁업체에게 정보시스템을 위탁하여 운영할 때에 다음사항이 포함된 정보시스템 위탁운영계획서를 제출하여 받아 사전 검토

- 위탁개요(위탁내용, 위탁업체 · 비용 · 기간, 운영인력 등)
- 정보통신망 구성현황 및 보안대책(보안체계의 세부내역 포함)
- 위탁시스템의 개인정보 보유현황 및 보호대책
- 운영효율 향상 및 서비스 개선 방안(기반시스템 공동 활용, 서비스수준협약서 등)
- 위탁운영비 세부산출 내역
- 위탁시스템에 대한 향후 추진계획(시스템 고도화 등)
- 기타 보안 대책

3. 외주인력 통제 강화 방안

○ 외주인력으로 인한 내부정보 유출 등 보안위협을 통제하기 위해 고려해야할 정보보호 실행지침은 크게 ① 물리적 대책, ② 인적보안관리, ③ 관리적 대책, ④ 기술적 대책 등 4단계로 구분

가. 물리적 대책

○ 중요정보가 보관된 장소에 대한 외주인력의 접근 통제와 같은 물리적 보안 대책

정보보호 활동	세부 내용
1) 물리적 접근통제	• 외주인력의 정보시스템, 정보보관소 접근 통제 • 필요 시 접근 유형 및 접근 사유 파악 • 제한구역, 접견구역, 장비출하구역 등을 구분하여 보안조치와 절차 수립
2) 출입이력 관리	• 출입이력 관리대장 사용 • 접근통제의 방법과 범위 등을 문서화
3) 이동매체 반 · 출입통제	• 반 · 출입되는 이동매체에 대한 파악 • 이동매체 반 · 출입 과정의 문서화 • 반 · 출입되는 이동매체의 보안검사

1) 물리적 접근 통제

○ 보호 필요 시설 및 장비에 대한 권한 없는 자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 보호하기 위한 보호구역 정의 및 이에 따른 보안대책 수립

- 제한구역, 접견구역, 장비출하구역 등을 별도로 지정하여 각각에 적합한 보안 조치와 절차 수립

○ 접근통제 절차에 포함되는 사항

- 물리적 보호구역의 중요도에 따라 접근통제 정도의 명시
- 접근통제 방법 명시(카드 센서 장치, IC카드, 광카드, 출입관리장치, 암호입력장치, 생체인식장치 등)

- 정보시스템 및 중요시설에 대한 물리적 접근통제 방법 기록

2) 출입이력 관리

○ 외주인력이 업무수행을 목적으로 보안구역에 출입할 때 출입내역 관리대장과 같은 출입내역을 확인할 수 있는 대책 수립

○ 출입이력 관리방안

- 접근통제가 요구되는 업무를 정의하고, 이 업무에 대한 접근통제의 방법과 범위 등을 문서화
- 외부인 출입 시 출입자, 출입시간, 출입목적에 대한 내용을 기록하고 관리
- 출입자 기록의 재검토(시설 보안등급에 따른 출입자 권한, 출입 목적, 출입시간의 적정성)

3) 이동매체 반 · 출입 통제

○ 외주인력이 반입하는 이동매체의 악성코드 감염 및 중요정보를 이동매체에 저장 후 반출하여 중요정보의 유출 위협

○ 외주인력이 반입하는 이동매체에 악성코드가 감염되어 내부 시스템에 피해를 입히거나, 내부 중요정보를 이동매체에 저장하여 반출하는 경우 중요정보가 유출되는 위협이 존재

○ 내부사용 이동매체의 관리 방안

- (관리자 지정) 보조기억매체 관리책임자 및 정보보안담당관 지정
  · 관리책임자 : 관리대장 등록현황 유지, 수량 및 보관상태 점검, 반출 · 입 통제, 사용 감독 등
  · 정보보안담당관 : 관리기관의 보조기억매체 등록 현황 파악, 보조기억매체 라벨 작성, 미등록 매체에 업무자료 보관 및 비밀보관 매체의 무단반출 인지 시 경위조사 · 조치
- (매체 도입절차) 보조기억매체 도입 시 국정원 보안적합성 검증을 거친 제품을 도입
- (매체 관리) 보조기억매체는 관리대장에 등재 후 사용
  · 보조기억매체는 일반용, 비밀용(대외비용), 공인인증서 보관용으로 구분하여 사용 · 관리
- (사용제한) 보조기억매체는 업무목적 이외 사적인 용도로 임의 사용을 제한하고 주기적인 점검 실시

- (불용처리 및 재사용) 불용처리 시 물리적 파기 후 관리대장에 기록 · 관리하고, 용도를 전환하여 재사용 시 파일 삭제, 포맷 및 파일복원 방지대책 강구

- (분실 시 대처 방안) 관리책임자 및 정보보안담당관에게 즉시 통지하고, 경위 조사를 통해 재발방지 대책 강구

- (고장 · 훼손, 오인 삭제 시 대처방안) 불용처리를 원칙으로 하나, 자료복구 필요 시 전문업체 의뢰 가능

나. 인적 보안관리

○ 외주인력 통제를 위한 외주인력 신원확인 등과 같은 인적보안관리

정보보호 활동	세부 내용
1) 상주 유지보수 인력 신원확인	• 외주인력의 사전 신원확인 • 보안서약서 작성 • 보안의식 강화를 위한 보안교육 실시
2) 현장 동행	• 보안구역 출입관리 대장 • 외부인이 출입제한 구역에 출입할 경우 보안관리자와 동행

1) 상주 유지보수 인력 신원확인

○ 상시 유지보수 인력으로 배치되는 인력에 대한 사전 신원확인을 시행하여 적합한 인력인지를 사전에 확인

- 상시 유지인력에 대한 보안서약서 작성 및 보안교육 실시

2) 현장 동행

○ 유지보수를 위한 외주업체 직원의 출입 또는 기타 부득이한 사유로 출입이 필요할 경우 내부 인가자의 동행 하에 출입

- 출입자는 출입관리 대장에 신분, 목적 및 입실/퇴실 시간 기록

다. 관리적 대책

○정보시스템과 연관되어 있는 인원, 조직, 기술상에 대한 전반적이고 총체적인 보안대책

정보보호 활동	세부 내용
1) 작업내역 관리	• 외주인력의 내부시스템 접근 기록 상시 감독 • 저장매체 사용 방지를 위한 조치 실시
2) 시스템 접근권한관리	• 시스템 접근 라벨 정의 및 접근권한 개별 부여
3) 정보 시스템 관리	• PC 등과 같은 장비의 반입 전 초기화/점검 실시 • 보안SW 설치 • 외주인력에 대한 보안정책 수립 및 이행
4) 조직체계 정비 및 검사	• 용역업체의 보안 관리 계획 평가 • 입찰공고 이전에 투입 예상 자료 · 장비의 보안 요구기준 마련

1) 작업내역 관리

○ 외주인력의 작업 중 불필요한 저장 등을 통한 중요정보 유출 위협 존재

- 상시 유지인력에 대한 보안서약서 작성 및 보안교육 실시

○ 실행 지침

- 외주인력이 내부시스템 접근을 득한 경우 외주인력의 내부시스템 접근기록을 상시 감독하여 불법적인 접근을 방지
- 외주인력이 인 · 허가 받지 않은 저장매체를 이용하여 내부정보를 외부로 유출하는 것을 방지하기 위해 저장매체 반입을 제한하고, 매체기록 장치를 봉인

○ 유지보수를 위한 외주업체 직원의 출입 또는 기타 부득이한 사유로 출입이 필요할 경우 내부 인가자의 동행 하에 출입

- 출입자는 출입관리 대장에 신분, 목적 및 입실/퇴실 시간 기록

2) 시스템 접근권한 관리

○ 정보시스템에 접근할 수 있는 레벨을 사전에 설정하고 정보시스템 접근 목적에 따라서 접근권한을 개별 부여

3) 정보시스템 관리

○ 외주인력이 사용하는 정보 시스템에 악성코드 감염 예방 등관리적 보호대책 적용

○ 실행 지침

- (정보 시스템 통제) PC 등과 같은 장비의 반입 전 초기화(포맷)를 원칙으로 하나, 초기화가 어려운 경우 반드시 바이러스, 악성코드 등 PC점검 조치 후 사용

4) 조직체계 정비 및 감사

○ 외주인력에 대한 관리와 감사를 통한 관리적 보호대책 적용

○ (보안 관리 계획 마련) 제안서의 평가요소에 문서·시설·장비 등 보안관리 계획에 대한 평가항목 및 배점기준을 마련하고 제안요청서 작성 시 용역(아웃소싱)업체에 프로젝트 과정에 대한 보안 관리 계획을 요구

※ 보안 요구 기준 마련

- 입찰공고 이전에 투입이 예상되는 자료, 장비 가운데 보안이 요구되는 정보에 대하여 적정 보호등급으로 분류하여 보안요구기준 마련

- 웹호스팅 등 정보시스템을 위탁운영 시에는 해킹에 대비해 웹방화벽 등 관련 보안 시스템이 구비되어 있는지 여부와 단순 운영 이외 보안관리가 가능한지 여부를 검토

- 내부시스템 이용시간, 작업지역을 제한하여 접근통제를 실시

- 용역(아웃소싱)업체가 제시하는 자체 통제방법에 대하여 이를 평가하고 채택여부 등을 결정하며 필요시 추가적인 통제방안을 요구

라. 기술적 대책

○외주인력 통제를 위한 접근 통제와 저장 매체 통제 등의 기술적인 대책

정보보호 활동	세부 내용
1) 접근관리	• 내부시스템에 접근하여 수행한 작업 등을 확인할 수 있는 접근이력 관리시스템 운영 • 내부 시스템에 접근 시 두 가지 이상의 방법으로 사용자 인증 • 내부 시스템에 접근하는 기기에 대해 사전 점검
2) 출력물 유출방지	• 비공개 자료 출력 시 출력자, 출력일시 등을 기록
3) 네트워크 제한	• 외부망과 물리적 분리 • 내부 운영 시스템 별 논리적 망 분리 운영 • 네트워크를 통한 통신 시 암호화 적용
4) 반 · 출입 매체관리	• 용역업체의 보안 관리 계획 평가 • 입찰공고 이전에 투입 예상 자료 · 장비의 보안 요구기준 마련

1) 접근관리

○ 접근이력 관리를 통한 외주인력의 불법적인 접근여부를 감시

○ 실행 지침

- 접근이력 관리시스템 운영
- 내부시스템에 접근하여 수행한 작업 등을 확인할 수 있는 접근이력 관리시스템의 감사기록은 다음 항목을 포함

※ 접근이력 관리시스템 기능

- 사용자 ID
- 핵심 이벤트 일자, 시간, 기타 상세 정보
- 시스템 접근 시고의 성공과 거부 기록
- 데이터 및 기타 자원 접근 시도의 성공과 거부 기록
- 시스템 구성의 변경

- 권한의 사용
- 시스템 유틸리티와 어플리케이션의 사용
- 접근된 파일의 접근 유형
- 네트워크 주소와 프로토콜
- 접근이력 관리시스템에 의해 제기된 경고
- 바이러스 탐지 시스템 및 침입탐지시스템과 같은 보호시스템의 활성화 및 비활성화

2) 출력물 유출 방지

○ 중요정보가 인쇄된 출력물을 IT 외주인력이 불법적으로 반출하는 것을 방지하기 위한 보호대책 적용

○ 실행 지침

- IT 외주인력에게 제공한 출력물 관리
- 비공개자료 출력 시에는 출력물에 출력자, 출력일시 등을 표시

3) 네트워크 제한

○ 외주인력의 네트워크 접근 제한 등과 같은 보안 대책

○ 실행 지침

- 물리적 망 분리 운용
  · 네트워크관리자는 비밀을 취급하는 네트워크를 외부망과 분리 운용
  · 내부망과 외부망 연동 시 효율적인 보안관리를 위하여 연결지점을 최소화 운용
- 논리적 망 분리 운용
  · 인터넷서비스망, 업무전산망, PC 영역 등의 영역으로 분리
  · PC, 서버, 데이터 등 정보시스템을 물리적으로 분리된 인터넷 서비스망과 업무전산망 영역으로 분리
  · 홈페이지 및 공개 서버의 경우는 내부 네트워크와 분리하여 DMZ에 구성
  · 외주인력 등을 활용할 경우에는 내부 네트워크와 분리된 네트워크로 구성

- 데이터 통신 보안
  · 네트워크상에서 이루어지는 통신을 안전하고 신뢰할 수 있도록 하기위해 통신내용 암호화 적용

4) 반 · 출입 매체관리

○ 외주인력이 반출 · 입하는 장비 및 매체에 대한 보호대책 적용

○ 실행 지침

- 반출 · 입 매체의 악성코드 검사
- 반출 · 입 매체의 통제
  · 외주 인력의 업무에 불필요한 매체에 대한 압수 보관
  · 외주 인력이 반출하는 저장매체의 내부에 저장된 자료 검사
- 이동매체 제한 및 관리를 위한 자동화된 시스템 도구의 도입

〈 외주용역 유형별 보호대책 (필수 : ○, 옵션 : △, 해당사항 없음 : ×) 〉

외주용역 유형	물리적 대책			인적 보안 관리		관리적 대책				기술적 대책			
	접근통제	출입이력관리	이동매체통제	신원조회	현장동행	작업내역관리	접근권한관리	정보시스템관리	조직체계관리	접근관리	출력물관리	네트워크제한	매체관리
운영 용역	○	△	○	○	△	○	○	○	○	○	○	○	○
유지 보수 용역	○	○	○	○	○	○	○	○	○	○	○	○	○
SI 용역	○	△	○	○	△	○	○	○	○	○	△	○	○
데이터 처리 용역	X	X	X	X	X	○	○	○	○	○	○	○	○
오프라인 지원	X	X	○	○	X	○	△	○	○	X	○	△	△

〈 최근의 개인정보 유출사례 〉

○ **(경위)** 코리아크레딧뷰로*(KCB)의 직원이 카드 3사의 위 · 변조 방지시스템의 **용역과정(1년 2개월)에서 카드사의 고객정보(약 1억건**)를 외부에 유출** ('12.12월~'13.12월)

- 유출된 1억여 건 가운데 7천 7백만 건을 천 6백여만 원을 받고 광고대행업자에게 팔았음

* IMF 이후 신용불량자 문제 등을 해결하고자 2005년, 신용조회 및 신용조사 업무 등을 하는 19개 금융회사의 공동출자한 KCB가 설립

** KB카드 약 5,300만 건, NH카드 약 2,500만 건, 롯데카드 약 2,600만 건

○ **(원인)** 외부인의 USB사용 차단, 고객정보 암호화 등 안전성 **준수사항을 카드 3사들이 불이행**

- 보안 프로그램이 해제된 상태에서 데이터에 접근할 수 있는 권한을 악용해서 관련 정보*를 **USB메모리에 복사**

* 정보 : 이름, 주민번호, 직장 주소, 이용한도, 이메일, 카드결제계좌, 카드결제일, 직장전화, 직장정보, 자택전화, 주거상황, 카드신용등급 등

○ **(문제점)** 해당 카드 3사들은 검찰 수사가 시작되기 전까지 정보유출에 대해 전혀 인식하지 못하였음

- 외부 회사의 직원이 혼자서 전산망에 접속했는데도 카드 3사들이 **감독을 제대로 하지 않아 범행이 가능**

○ **(대책)** 외주용역 시 **물리적, 인적, 관리적 및 기술적 보안** 체계 유지

〈 물리적, 인적, 관리적 및 기술적 보완 대책 〉

■ 물리적 보안대책

o 외주용역 업체의 근로자는 퇴근할 때 지정된 **파쇄장비**를 이용하여 **복사, 출력 등 자료를 완전파기 후 퇴근**

o 외주용역 업체의 근로자 등이 노트북, USB메모리 등 행정자료의 유출을 쉽게 할 수 있는 **저장매체 등 반입 금지**

■ 인적 보안대책

o 행정자료의 행정자료통합관리시스템에 **적재, 고유식별번호의 암호화** 등 핵심내용은 지정된 **공무원이 담당**하고 **시스템 개발, 유지 · 보수** 등 기타 업무는 **외주용역 업체의 직원이 담당**

■ 관리적 보안대책

o 행정자료의 보안을 담당하는 **관리책임관**을 지정하여 운영

- 관리책임관의 행정자료의 적재 · 보관 · 처리 · 공표 · 제공 전반에 대한 **보안 관리 강화**
- 관리책임관은 행정자료의 **이용자 최소화** 및 보안이행 점검 프로세스를 강화하고, 보안규정 준수여부를 **수시로 점검**

o 통계청은 **통계작성기관**의 장이 표본 추출용 행정자료에 대한 **보안 서약서의 준수여부 및 사후 파기**를 **확인하고 점검**

■ 기술적 보안대책

o 모든 행정자료를 행정자료통합관리시스템에 적재한 후 원격분석 시스템을 통해 이용(**개인 PC 등에 저장 불가**)

o 외주용역 업체 근로자 등의 시스템 **접속기록을 실시간 확인하고 점검하는 모니터링 구축 및 운영**

o 외주용역 업체의 시스템 개발, 유지 · 보수 등에 필요한 장비는 **통계청이 일괄 제공**

PART VI

행정자료를 이용한 국가통계 작성 표준편람(II)

참 고

참고1

「개인정보보호법」과 「통계법」과의 관계

함께하는 공정사회! 더 큰 희망 대한민국!

행 정 안 전 부

수신자 통계청장(행정자료관리과장)
(경유)
제목 **개인정보보호법령 질의 회신(통계청)**

귀 청 행정자료관리과-17(2012.1.4.)호와 관련하여 아래와 같이 회신 드리오니 업무에 참고하시기 바랍니다.

1. 질의요약

통계법 제24조(행정자료의 제공)의 규정에 의거하여 통계청이 농림수산식품부에 주민등록번호 등 개인정보가 포함된 행정자료(홍성군 농업경영체 등록자료)를 요청하여 수집하는 경우에도 개인정보보호법 제24조가 적용되는지 여부

2. 답변내용

통계법에 따라 수집되는 개인정보는 개인정보보호법 제58조제1항제1호에 따라 제3장부터 제7장(같은 법 제15조부터 제57조까지를 말함)까지 적용이 제외되므로, 주민등록번호가 포함된 행정자료를 수집하는 경우에도 같은 법 제24조가 적용되지 않습니다. 끝.

행정안전부장관

주무관 정종일 행정사무관 서상우 개인정보보호 전담 이/07 과장 유영님

시행 개인정보보호과-66 (2012. 01. 09.) 접수 행정자료관리과-41 (2012. 01. 09.)

우 110-760 서울특별시 종로구 세종대로 209 / http://www.mopas.go.kr

전화 02-2100-3615 전송 02-2100-1739 / jijung@mopas.go.kr / 비공개(6)

서민을 따뜻하게, 중산층을 두텁게

참고2

행정자료의 정보보호를 위한 운영규정

제　　정 통계청예규 제48호 2009. 1. 7.
개　　정 통계청예규 제58호 2009. 9.25.
일괄개정 통계청예규 제62호 2010. 3.25.
개　　정 통계청예규 제70호 2011. 7.22.

제1장 총 칙

제1조(목적) 이 규정은 "통계법"(이하 "법"이라 한다), 같은 법 시행령에 따른 행정자료의 접수, 보관 및 활용에 있어서 개인이나 법인 또는 단체 등의 정보를 보호 함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "행정자료"란 법 제24조제1항에 따른 행정자료를 말한다.
2. "정보보호조치"란 행정자료에 포함되어 있는 개인, 법인 또는 단체 등의 정보를 보호하기 위하여 행하는 사용방법 및 사용부서 등에 대한 제한 및 그 밖의 보안조치를 말한다.
3. "개체식별정보"란 행정자료내의 주민등록번호, 사업자등록번호 또는 성명 · 명칭 등 개체를 식별할 수 있는 항목을 말한다.
4. "개체식별자료"란 개체식별정보를 포함하고 있는 행정자료를 말한다.
5. "개별파일"이란 DB화되지 않은 파일 형태의 행정자료를 말한다.
6. "행정자료 DB"란 행정자료를 수록한 데이터베이스 등을 말한다.
7. "온라인"이란 자료요청기관이 접속권한을 부여받아 자료제공기관의 시스템에 직접 접속하여 실시간으로 자료를 내려 받거나 자료제공기관이 자료요청기관의 시스템에 접속하여 실시간으로 전송하는 데이터처리시스템 및 이에 준하는 것을 말한다. 〈개정 2011. 7.22〉
8. "오프라인"이란 해당 행정자료를 직접 제공 또는 접수하기 위한 인편 등의 수단을 말한다.

제3조(적용범위) ① 이 규정은 통계청과 통계교육원, 통계개발원, 지방통계청(이하 '소속기관'이라 한다)에 적용한다. 〈개정 2011. 7.22〉

② 통계청과 그 소속기관이 통계작성 목적으로 법 제24조에 따른 공공기관(이하 "자료제공기관"으로 한다)으로부터 개체식별자료(이하 "자료"라 한다)를 접수해서 보관, 활용에 이르는 모든 과정을 포함한다. 〈개정 2011. 7.22〉

제2장 행정자료의 접수 및 관리

제4조(자료관리책임자) ① 통계청장은 자료의 유출 · 변경 · 파괴 등을 방지하기 위하여 정보화 기획과장을 자료관리책임자로 지정하여야 한다. 〈개정 2011. 7.22〉

② 자료관리책임자는 다음 각 호의 업무를 수행하여야 한다.

1. 자료의 접수
2. 자료의 관리
3. 자료이용자의 인가 및 관리
4. PC의 지정 및 관리
5. 접속기록 등의 관리
6. 자료의 제공
7. 보안지도 등 그 밖의 정보보호조치를 위하여 필요한 사항

③ 지방통계청(사무소를 포함한다. 이하 지방통계청이라 함) 조사지원과장을 자료관리분임책임자로 지정하여 지방통계청에서 접수한 모든 자료에 대하여 자료관리책임자 업무를 대행하게 할 수 있다. 〈신설 2011. 7.22〉

④ 자료관리책임자는 제2항 각 호의 업무를 효율적으로 수행하기 위하여 자료관리담당자를 지정할 수 있다. 〈개정 2011. 7.22〉

⑤ 자료관리분임책임자는 지방통계청에서 입수 및 보관, 활용하는 자료에 대하여 제2항 각 호의 업무를 효율적으로 수행하기 위하여 자료관리분임담당자를 지정할 수 있다. 〈신설 2011. 7.22〉

제5조(접수방법) ① 자료제공기관으로부터 자료의 접수는 자료관리책임자가 일괄하여 수행하여야 한다. 다만, 소관부서가 접수하는 것이 필요하다고 자료관리책임자가 판단하는 경우에는 소관부서의 자료관리담당자를 지정하여 해당 자료를 접수하게 할 수 있다.

② 제1항 단서에 따라 자료를 접수한 소관부서는 특별한 사유가 없는 한 접수 후 지체 없이 해당 자료를 자료관리책임자에게 인계하여야 한다.

③ 지방통계청 업무망과 인터넷망 분리시점까지 자료관리책임자는 자료관리분임책임자에게 지방통계청에서 접수한 행정자료의 일부 또는 전부를 관리하도록 위임할 수 있다. 다만 자료관리분임책임자는 정기적으로 접수되는 자료에 대해서는 별첨 제1호의 서식에 의해 반기 1회 이상 보고하여야 하며, 신규 접수 또는 변동사항이 많은 자료에 대해서는 접수 즉시 자료관리책임자에게 보고하여야 한다. 〈신설 2011. 7.22〉

④ 자료의 접수는 온라인을 통한 접수를 원칙으로 한다. 다만, 자료제공기관이 오프라인을 통한

자료접수를 요구하는 경우 자료관리책임자는 자료제공기관과 구체적인 접수방법 및 저장매체 등을 협의할 수 있다. 〈개정 2011. 7.22〉

⑤ 제2항 단서의 오프라인을 통한 자료의 접수 시 접수매체는 다트 데이프(DAT TAPE)나 "USB메모리 등 휴대용 저장매체 보안관리지침" 제4조에 따라 보안적합성 검증을 필한 USB메모리 또는 이에 준하여 보안성이 인정되는 것으로 제한한다. 〈개정 2011. 7.22〉

제6조(자료보관) ① 통계청장은 접수한 행정자료를 계속적으로 활용하기 위하여 행정자료 DB(이하 "DB"라 한다)를 구축하여야 한다. 다만, DB구축 이전 또는 자료의 DB화를 위한 처리기간 및 자료제공기관의 요구 등 특별한 사유가 있는 경우 개별파일 형태로 보관할 수 있다. 〈개정 2011. 7.22〉

② 제1항 단서의 개별파일을 DB화한 이후에는 해당 파일을 복구할 수 없는 방법으로 파기하여야 한다. 자료제공기관이 자료에 대해 활용 후 폐기를 요구하는 경우에도 이와 같다.

제7조(자료관리) ① DB를 구축하여 자료를 보관ㆍ활용하는 경우 자료관리책임자는 자료의 등록부터 폐기까지의 모든 이력을 DB에서 관리하여야 한다. 다만, DB 관리프로그램이 설치되기 이전까지는 별첨 제1호의 서식으로 관리할 수 있다.

② 자료를 개별파일 형태로 보관하는 경우 자료관리책임자는 등록부터 폐기까지의 모든 이력을 별첨 제1호의 서식으로 관리하여야 한다. 관리부서의 변경으로 자료를 이관하는 경우에는 동 관리대장을 같이 이관하여야 한다.

③ 통계청장은 자료제공기관이 제1항과 제2항에 따른 자료관리 현황에 대해 열람을 요구하는 경우 이에 따라야 한다. 〈개정 2011. 7.22〉

제3장 행정자료의 활용

제8조(자료접근권자) ① 통계작성을 목적으로 자료를 이용하고자 하는 자는 별첨 제3호의 서식의 서약서 및 별첨 제4호의 서식의 자료이용신청서를 작성하여 자료관리책임자에게 제출하여야 한다.

② 자료관리책임자는 소관업무 및 자료의 사용목적 등을 종합적으로 심사하여 해당 자료에 접근ㆍ처리할 수 있는 자(이하 "자료접근권자"라 한다)를 다음 각 호에 따라 인가하고 별첨 제5호의 서식을 통해 자료접근권자를 관리하여야 한다.

1. 정기자료접근권자 : 업무의 속성상 정기적으로 자료에의 접근이 필요한 자로 소관업무의 수행기간동안 접근권한을 부여

2. 수시자료접근권자 : 일시적으로 자료에의 접근이 필요한 자로 해당기간을 정하여 접근권한을 부여

제9조(자료처리) ① 자료접근권자는 자료관리책임자가 지정한 PC(이하 "지정PC"라 한다)를 통해서만 제8조제2항에 따라 인가된 자료에 대하여 비교 · 분석 · 생성 등 자료처리를 할 수 있다.

② 자료관리책임자는 지정PC에의 접속을 효과적으로 제한하기 위하여 전자정부법 제20조에 따른 행정전자서명으로 본인임을 확인하여야 한다.

③ 자료관리책임자는 자료접근권자가 자료처리과정에서 개체식별자료를 다운로드 또는 저장("화면캡쳐"를 포함한다)할 수 없도록 관련 프로그램을 설치하여야 한다.

④ 자료접근권자는 자료에 대한 활용이 종료되는 대로 자료의 활용과정에서 생성된 것으로서 개체식별정보 또는 개체식별자료가 기록된 인쇄물 및 전자파일 등 생성자료를 복구할 수 없는 방법으로 폐기하여야 한다.

제10조(접속기록의 관리 및 보관) ① 자료관리책임자는 자료접근권자가 지정PC에 접속하여 자료처리한 내역(이하 "접속기록"이라 한다)을 관리하기 위하여 다음 각 호의 사항을 자동적으로 기록할 수 있는 관련 프로그램을 지정PC에 설치하여야 한다.

1. 자료접근권자의 성명 · 소속 · 직급
2. 자료접근권자가 활용한 자료의 명칭 및 작업내용
3. 접속시간
4. 제9조제4항이 정하는 생성자료의 명칭 · 크기 · 보관매체
5. 제9조제4항에 따른 자료처리 후 조치결과 등

② 제1항에도 불구하고 지정PC에 관련 프로그램을 설치하기 이전까지는 별첨 제6호의 서식에 따른 작업일지 및 별첨 제7호의 서식에 따른 생성자료관리대장을 통해 접속기록을 관리 · 보관할 수 있다.

③ 자료관리책임자는 제1항 및 제2항에 따른 접속기록을 3년 이상 상시 보관하고 접속기록의 이상 유무 등을 분기 1회 이상 점검하여야 한다.

④ 통계청장은 자료제공기관이 접속기록에 대해 열람을 요구하는 경우 이에 따라야 한다.
〈개정 2011. 7.22〉

제11조(개별파일의 제공) ① 자료관리책임자는 개별파일 형태로 보관중인 자료에 대해 통계작성 목적으로 활용하고자 하는 부서 등(이하 "자료활용부서"라 한다)에 제공할 수 있다.

② 제1항에 따라 자료관리책임자가 자료활용부서에 자료를 제공하는 경우 다음 각 호의 정보보호조치를 해야 한다.

1. 제5조 제4항이 정하는 보조기억매체의 이용
2. 별첨 제1호의 서식의 자료관리대장의 기록

3. 별첨 제2호의 서식의 자료제공대장의 기록

4. 별첨 제3호의 서식의 서약서 및 별첨 제4호의 서식의 서약서 징구

5. 자료관리담당자 지정

③ 자료활용부서장은 인수한 자료의 활용기간 동안 자료관리책임자의 관리의무에 준하여 이를 관리하여야 한다.

④ 자료관리책임자는 제3항에 따른 자료활용부서의 자료관리 현황을 점검하고 필요시 적절한 정보보호조치를 취하도록 요구할 수 있다.

⑤ 자료활용부서장은 인수한 자료를 통한 활용이 종료하는 즉시 인수한 자료는 반납하고 개체식별정보나 개체식별자료가 기록된 인쇄물 및 전자파일 등 생성자료는 복구할 수 없는 방법으로 폐기하여야 한다. 〈개정 2011. 7.22〉

제4장 행정자료 보안지도 · 감사 · 조사 및 교육

제12조(보안지도 및 점검) ① 자료관리책임자는 자체 및 소속기관의 자료관리 실태를 확인, 개선대책을 마련하기 위하여 연 1회 이상 보안지도 및 점검을 실시하여야 한다.

② 자료관리책임자가 제1항에 따라 보안지도 및 점검시 확인해야 할 사항은 다음 각 호와 같다.

1. 제5조제2항과 관련하여 소관부서가 해당 자료를 자료관리책임자에게 인계시 지연여부

2. 오프라인을 통한 자료 접수시 제5조 제4항에서 정한 이외의 접수매체의 이용여부 〈개정 2011. 7.22〉

3. 제6조 제2항이 정하는 개별파일의 폐기여부

4. 제7조 제1항 및 제2항에 따른 자료 관리의 이상 유무〈개정 2011. 7.22〉

5. 제8조 제2항에 따라 인가받은 목적 이외의 자료의 이용여부

6. 제9조 제4항이 정하는 개체식별정보가 포함된 생성자료의 폐기여부

7. 제10조 제2항에 따른 접속기록의 이상 유무

8. 제11조 제3항에 따른 자료활용부서장의 관리의무 준수여부

9. 그 밖의 정보보호조치를 위하여 필요한 사항

③ 보안점검은 정기점검과 수시점검으로 구분하여 실시한다. 다만, 정기점검은 보안감사로 갈음할 수 있다.

④ 자료관리책임자는 보안지도 및 점검 결과 도출된 미비점을 시정 · 보완하기 위한 개선대책을 마련하여야 한다.

⑤ 자료관리책임자는 제1항에 따른 보안지도 · 점검계획 및 결과를 통계청장에게 보고하여야 한다. 〈개정 2011. 7.22〉

제13조(보안감사) 통계청장은 보안업무규정 시행세칙 제121조에 따른 정기보안감사에 자료관리 보안업무를 포함하여 실시하여야 한다. 〈개정 2011. 7.22〉

제14조(보안교육) 「보안업무규정 시행세칙」 제7조에 따른 정보보안담당관은 자체 및 소속기관의 행정정보 활용업무 취급자를 대상으로 연 1회 이상 순회 또는 소집 보안교육을 실시하여야 한다. 다만, 「보안업무규정 시행세칙」 제120조에 따른 정보보안 교육으로 갈음할 수 있다.

제15조(보안사고에 대한 조치) ① 규정 제4조에서 제6조까지의 규정과 제9조에서 제11조까지의 규정에서 정한 사항을 범한 자 또는 이를 인지하거나 발견한 자는 즉시 피해를 최소화하는 조치를 취하고 사고일시 및 장소, 사고내용을 가장 신속한 방법으로 보안담당관 및 정보보안담당관에게 보고하여야 한다.

② 제1항의 보고를 받은 보안담당관은 지체 없이 그 내용을 통계청장에게 보고 및 국가정보원장에게 통보한 후 자체조사를 실시하여야 한다. 〈개정 2011. 7.22〉

③ 통계청장은 조사결과에 따라 관련자를 문책하고 재발방지를 위한 대책을 마련하여 국가정보원장 및 자료제공기관장에게 통보하여야 한다. 〈개정 2011. 7.22〉

제5장 보 칙

제16조(준용) 이 규정에 명시되지 않은 사항은 다음의 관련 규정 및 지침에 따른다.

1. 보안업무규정 및 동 시행규칙
2. 통계청 보안업무규정 시행세칙
3. 국가 사이버안전 관리규정
4. 국가 정보보안 기본지침
5. 행정자치부 공공기관 개인정보보호 기본지침
6. 행정기관 정보시스템 접근권한 관리 규정
7. USB메모리 등 휴대용 저장매체 보안관리지침 〈개정 2011. 7.22〉
8. 통계청 정보시스템 저장매체 불용처리지침

9. 보존용 전산자료 관리 및 이용 지침

10. 정보자산 보안관리 지침

11. 그 밖의 관련법령

부칙 〈2009. 1. 7〉

동 규정은 발령 후 3개월이 경과한 날부터 시행한다.

부칙 〈2009. 9.25.〉

동 규정은 발령한 날부터 시행한다.

부칙 〈2010. 3.25.〉

이 지침은 공포한 날부터 시행한다.

부칙 〈2011. 7.22.〉

제1조(시행일) 이 예규는 공포한 날부터 시행한다.

[별첨 제1호 서식]

자료관리대장

자료명	주요 수록내용	건수	자료접수			형태	보관장소	자료 폐기/이관		관리 책임자
			제공기관	문서번호	일자			문서번호	일자	

* 주요 수록내용 : 자료를 구성하는 주요 항목
* 건수 : 자료를 구성하는 데이터수
* 형태 : 수록매체명(USB 등), 파일프로그램명(text, 엑셀 등)
* 보관장소 : 행정정보팀 비밀보관 캐비닛 등
* 관리책임자 : 행정자료 통계목적 활용 담당사무관 성명

[별첨 제2호 서식]

자료제공대장

□ **자료명 :**

번호	요청문서 번호(일자)	제공문서 번호(일자)	제공부서	수령자	활용목적	제공형태	반납일	확인

* 요청문서번호(일자)에는 요청기관이 보낸 공문의 번호와 시행일자 기록
* 제공문서번호(일자)에는 제공한다는 공문의 번호와 시행일자 기록(공문을 보내지 않을 경우 제공일자만 기록)
* 수령자에 대해서는 서약서 징구
* 제공형태 : USB메모리 등
* 확인 난에는 담당자 이름 기재

[별첨 제3호 서식]

서 약 서

행정자료명 :

제공내용 : 예시) 수록데이터 건수, 매체형태 등

본인은 통계 목적으로 활용하기 위해 위 행정자료를 인수 · 처리함에 있어 통계법 제33조와 제34조 등의 비밀보호 관련 제 규정을 준수합니다. 이에 따라 본인과 소속부서(　　)는 동 자료에 수록된 개인 또는 법인이나 단체의 개체식별 정보가 유출되지 않도록 동 자료의 처리과정에서 생성된 자료의 폐기 등을 포함하여 자료관리 전반에 철저를 기하겠습니다. 만약 자료가 외부에 유출되었을 때에는 당사자로서 규정에 따른 처벌을 받는데 이의 없음을 엄숙히 서약합니다.

20 년 월 일

서약자 소속 :

직급 :

성명 :

[별첨 제4호 서식]

자료 이용신청서

과 장

※자료소관부서의장

담 당	사무관	과 장

소 속 과		직 위		성 명	
이용기간			비 고	정기, 수시	
행정자료명 :					
사용목적 :					

[자료이용시 준수사항]

– 자료이용과정에서 알게 된 비밀에 속하는 사항에 대한 누설금지

– 통계작성 목적 이외의 활용금지

위의 자료이용시 준수사항을 지킬 것을 약속하며 해당 행정자료의 이용을 신청합니다.

년. 월. 일.

신청자 : 인

[별첨 제5호 서식]

자료접근권자 관리대장

【정기자료접근권자】

관리번호	성명	직급	소속/담당업무	인가기간	사용목적
1					
2					
3					
4					
5					
6					

【수시자료접근권자】

관리번호	성명	직급	소속/담당업무	인가기간	사용목적
1					
2					
3					
4					
5					
6					

[별첨 제6호 서식]

작업일지

행정자료명 :

부서명 :

일시	작업내용	파일접근자			확인자
		성명	소속 · 직급	서명	
월 일 시 분 ~ 시 분					

* 부서별로 관리
  - 파일(원본 및 파생파일)에 접근한 사람은 모두 기록
* 작업내용 : 파일 복사, 변환, 열람 등

[별첨 제5호 서식]

생성자료 관리대장

부서명 :

생성일자 (출력일자)	파일명(확장자 포함)/생성물명	크기 및 보관매체	작업자		작업후 조치	
			성명	소속 · 직급	조치내용	조치일자

* 자료활용 부서용
* 크기 : KB, MB 등(파일), 페이지 수(생성자료)
* 보관매체(파일에만 해당) : USB 등
  ⇒ 반드시 부서내 등록된 매체 활용
* 조치내용 : 파일 삭제, 출력물 폐기 등

참고3

통계청 개인정보보호지침

제　　정 통계청예규 제 83호 2012. 8.30.
일괄개정 통계청예규 제103호 2013. 4. 2.

제1장 총　칙

제1조(목적) 이 개인정보 보호지침(이하 "지침"이라 한다)은 「개인정보 보호법」(이하 "법"이라 한다) 에 따라 개인정보보호에 필요한 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보 처리"란 개인정보를 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
2. "개인정보처리자"란 개인정보를 처리하는 모든 공공기관, 영리목적의 사업자, 협회 · 동창회 등 비영리기관 · 단체, 개인 등을 말하며, 이 지침에서는 "통계청"을 지칭한다.
3. "공공기관"이란 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체와 그 밖의 국가기관 및 공공단체 중 대통령령으로 정한 기관을 말한다.
4. "친목단체"란 학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 각종 동창회, 동호회, 향우회, 반상회 및 동아리 등의 모임을 말한다.
5. "개인정보 보호책임자"란 통계청의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 에 따른 지위에 해당하는 자를 말한다.
6. "개인정보보호 업무담당자"란 개인정보보호에 관한 업무를 행정적으로 청 전체를 총괄하여 실무를 담당하는 자를 말한다.
7. "부서별 개인정보보호 업무담당자"란 개인정보보호에 관한 업무를 행정적으로 소속 부서 전체를 총괄하여 실무를 담당하는 자를 말한다.
8. "개인정보취급자"란 통계청의 업무를 수행함에 있어 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에

접근하여 처리하는 모든 자를 말한다.

9. "개인정보처리시스템"이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템을 말한다.

10. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유 · 무선망을 통하여 전송하는 일체의 장치로서 폐쇄회로텔레비전(CCTV) 및 네트워크카메라를 말한다.

11. "개인영상정보"라 함은 영상정보처리기기로 촬영 · 처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.

12. "영상정보처리기기 운영자"라 함은 개인정보 보호법에 따라 영상정보처리기기를 설치 · 운영하는 자를 말한다.

13. "공개된 장소"라 함은 공원, 도로, 지하철, 상가 내부, 주차장 등 정보주체가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

14. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

15. "제3자"란 정보주체와 정보주체 또는 그의 법정대리인으로부터 개인정보를 실질적 · 직접적으로 수집 · 보유한 개인정보처리자를 제외한 모든 자를 의미하며, 개인정보처리자로부터 개인정보처리 업무를 위탁받아 처리하는 자(이하 "수탁자")는 제외한다.

제3조(적용범위) 이 지침은 전자적 처리 여부를 불문하고 수기문서를 포함한 모든 형태의 개인정보파일을 운용하는 통계청과 통계교육원, 통계개발원, 지방통계청(이하 '소속기관'이라 한다)의 직원 및 계약관계에 있는 외주 직원에게 적용된다.

제4조(개인정보 보호 원칙) ① 개인정보를 수집하는 목적은 수집 당시에 명확히 특정되어 있어야 하고 그 특정된 목적을 달성하기 위하여 직접적으로 필요한 범위에서만 개인정보를 처리하여야 한다.

② 개인정보의 내용이 처리당시의 사실에 부합하도록 정확하고 최신의 상태를 유지하여야 하며, 개인정보의 처리과정에서 고의 또는 과실로 개인정보가 부당하게 변경 또는 훼손되지 않도록 하여야 한다.

③ 정보주체의 권리가 침해받을 가능성과 위험의 정도에 상응하는 적절한 기술적 · 관리적 및 물리적 보안조치를 통하여 개인정보를 안전하게 관리하여야 한다.

④ 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 일반적으로 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차를 마련하여야 한다.

⑤ 처리 목적에 필요한 범위에서 개인정보를 처리하는 경우에도 가능한 한 정보주체의 사생활

침해를 최소화하는 방법을 선택하여야 한다.

⑥ 이 법에 따른 개인정보의 처리에 관한 정보주체의 동의를 얻은 경우라도 구체적인 업무의 특성상 가능한 경우에는 특정 개인을 알아볼 수 없는 형태로 개인정보를 처리하여야 한다.

제5조(다른 지침과의 관계) 통계청이 보유한 개인정보 중 통계법에 따라 수집된 행정자료 및 통계조사자료에 관해서는 본 지침이 적용되지 않으며, 「행정자료의 정보보호에 관한 규정」 및 「정보보안업무규정시행세칙」이 적용된다.

제2장 개인정보 처리 기준

제1절 개인정보의 처리

제6조(개인정보의 수집) ① 개인정보의 "수집"이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.

② 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체로부터 사전에 동의를 받은 경우
2. 법률에서 개인정보를 수집 · 이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보를 수집 · 이용하지 않고는 법령에서 부과하는 구체적인 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 공공기관이 개인정보를 수집 · 이용하지 않고는 법령 등에서 정한 소관업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
5. 개인정보를 수집 · 이용하지 않고는 정보주체와 계약을 체결하고, 체결된 계약의 내용에 따른 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
6. 정보주체 또는 그 밖의 모든 자의 생명, 신체, 재산에 대한 피해를 방지해야 할 급박한 상황이어서 개인정보를 수집 · 이용해야 할 필요성이 명백히 인정됨에도 불구하고 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 연락을 취할 수 없는 상황이어서 사전에 동의를 받을 수 없는 경우
7. 개인정보처리자가 법령 또는 정보주체와의 계약에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 개인정보의 수집 · 이용에 관한 동의 여부 및 동의 범위 등을 선택하고 결정할 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집 · 이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 범위로 한정된다.

③ 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함 등"이라 함)를 제공받음으로써 개인정보를 수집하는 경우, 정보주체가 동의의사를 명확히 표시하거나 그렇지 않은 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위에서만 이용할 수 있다.

④ 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지등"이라 함)에서 개인정보를 수집하는 경우, 해당 개인정보는 본인의 개인정보를 인터넷 홈페이지등에 게시하거나 게시하도록 허용한 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위에서만 이용할 수 있다.

⑤ 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인으로부터 또는 의사표시를 하는 경우 대리인의 개인정보를 수집 · 이용할 수 있다.

⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」의 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집 · 이용할 수 있다.

제7조(정보주체의 사전 동의를 받을 수 없는 경우) 법에 따라 정보주체의 사전 동의 없이 개인정보를 수집, 이용 또는 제공한 경우, 해당 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집 또는 이용한 사실, 그 사유와 이용내역을 알려야 한다.

제8조(개인정보의 제공) ① 개인정보의 "제공"이란 개인정보의 저장매체 또는 개인정보가 담긴 출력물이나 책자 등의 물리적 이전, 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전과 공동으로 이용할 수 있는 상태를 초래하는 모든 행위를 말한다.

② 법에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제9조(개인정보의 목적 외 이용 등) ① 법에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 제공과 동시에 또는 필요한 경우 제공한 이후에 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.

② 법에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공하는 자와 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임관계를 명확히 하여야 한다.

③ 법에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

④ 법에 따라 개인정보를 제3자에게 제공하는 경우에는 다른 정보와 결합하여서도 특정 개인을 알아볼 수 없는 형태로 제공하여야 한다.

제10조(개인정보 수집 출처 등 고지) ① 정보주체 이외로부터 수집한 개인정보를 처리하는 경우 정당한 사유가 없으면 정보주체의 요구가 있은 날로부터 3일 이내에 개인정보의 수집 출처, 개인정보의 처리 목적, 법에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 정보주체에게 알려야 한다.

② 법에 근거하여 제1항에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없으면 정보주체의 요구가 있은 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제11조(개인정보의 파기방법 및 절차) ① 개인정보의 보유기간이 경과된 경우에는 정당한 사유가 없는 한 보유기간의 종료일로부터 5일 이내에, 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 5일 이내에 그 개인정보를 복원이 불가능한 방법으로 파기하여야 한다.

② '복원이 불가능한 방법'이란 사회통념상 현재의 기술수준에서 적절한 비용이 소요되는 방법을 말한다.

③ 개인정보의 파기에 관한 사항을 기록 · 관리하여야 한다.

④ 개인정보파기의 시행 및 확인은 개인정보 보호책임자의 책임하에 수행된다.

⑤ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.

⑥ 개인정보파일 파기에 관하여는 제59조 및 제60조를 적용한다.

제12조(법령에 따른 개인정보의 보존) 법에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 법령에 따라 해당 개인정보 또는 개인정보파일을 보존한다는 점을 분명히 표시하여야 한다.

제13조(동의를 받는 방법) ① 법에 따라 개인정보의 수집과 이용을 위하여 정보주체의 동의를 받고자 하는 경우에는 기본적인 재화 또는 서비스의 제공을 위하여 반드시 필요한 최소한의 개인정보와 부가적인 재화 또는 서비스의 제공을 위하여 필요한 최소한의 개인정보를 구분하여 정보주체에게 알리고 동의를 받아야 한다.

② 법에 따라 개인정보를 처리하기 위하여 정보주체의 동의를 얻고자 하는 경우에는 정보주체의 동의가 필요한 경우와 필요하지 않은 경우를 구분하고, 후자의 경우에는 정보주체의 동의 없이 개인정보를 처리할 수 있다는 점과 그 사유를 알려야 한다.

③ 법에 따라 정보주체로부터 별도의 동의를 받고자 하는 경우에는 정보주체가 다른 개인정보처리의 목적과 별도로 동의여부를 표시할 수 있도록 조치를 취하고 동의를 받아야 한다.

④ 「개인정보 보호법 시행령」(이하 "시행령"이라 한다)에 따라 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑤ 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 제1항에 의한 의무를 부담하지 아니한다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 그 밖에 친목단체의 구성원 상호간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항

제14조(법정대리인의 동의) ① 시행령에 따라 법정대리인의 성명 · 연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.

② 제1항에서 동의를 얻는 방법은 법에 따라 법정대리인으로부터 동의를 얻는 경우에도 적용된다.

③ 법에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 한다.

제15조(민감정보 처리) ① 법에 따라 민감정보의 처리를 위하여 정보주체에게 동의를 받고자 하는 경우에는 다른 개인정보와 민감정보를 구분하여 민감정보에 대하여는 정보주체가 별도로 동의할 수 있도록 조치를 취하여야 한다.

② 제1항에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 민감정보의 수집 · 이용 목적
2. 수집하려는 민감정보의 항목
3. 민감정보의 보유 및 이용 기간

4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제16조(고유식별정보 처리에 대한 동의) ① 법에 따라 고유식별정보의 처리를 위하여 정보주체에게 동의를 받고자 하는 경우에는 다른 개인정보와 고유식별정보를 구분하여 고유식별정보에 대하여는 정보주체가 별도로 동의할 수 있도록 조치를 취하여야 한다.

② 제1항에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 고유식별정보의 수집 · 이용 목적
2. 수집하려는 고유식별정보의 항목
3. 고유식별정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제17조(주민등록번호 이외의 회원가입 방법 제공) 시행령에 따라 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(이하 "대체수단"이라 한다)을 제공해야 하는 경우, 정보주체는 주민등록번호가 아닌 대체수단을 사용하여서도 회원으로 가입할 수 있다는 점을 회원가입절차를 위한 화면을 통하여 명시적으로 알리고 회원가입을 받아야 한다. 이 경우 주민등록번호를 이용한 회원가입 방법과 대체수단을 이용한 회원가입 방법을 하나의 화면을 통하여 제공하여야 한다.

제18조(개인정보취급자에 대한 감독) ① 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

② 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라 해당업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을 관리하기 위한 조치를 취해야 한다.

③ 개인정보취급자로 하여금 보안서약서를 제출하도록 하는 등 적절한 관리 · 감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

제2절 개인정보 처리의 위탁

제19조(수탁자의 선정 시 고려사항) ① 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 수탁자를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도,

책임능력 등을 종합적으로 고려하여야 한다.

② 개인정보의 처리 업무를 위탁하는 때에는 수탁자의 처리 업무의 지연, 처리 업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련하여야 한다.

제20조(개인정보 보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적 · 기술적 · 물리적 조치를 한다.

제21조(정보주체와 재위탁의 관계) ① 정보주체는 수탁자로부터 개인정보 처리 업무를 재위탁 받아 처리하는 자(이하 "재수탁자"라 한다)가 재위탁 받은 개인정보 처리 업무를 수행하면서 발생하는 손해에 대한 배상을 청구할 수 있다.

② 개인정보 처리 업무의 재위탁에 대해서는 법을 준용한다.

제3절 개인정보 보호책임자 및 취급자

제22조(개인정보 보호책임자의 지정) 통계청 전체의 개인정보보호책임자(CPO)는 통계정보국장으로 지정한다.

제23조(개인정보 보호책임자의 공개) ① 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 홈페이지에 공개하여야 한다.

② 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 다만, 개인정보 보호책임자와 개인정보 보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 기재할 수 있다.

제24조(개인정보 보호책임자의 역할 및 책임) 개인정보보호책임자의 역할 및 책임은 다음 각 호와 같다.

1. 개인정보보호계획 및 지침 수립
2. 개인정보보호 침해사례에 대한 신고처리 및 대응방안 수립
3. 개인정보보호계획 검토, 의견제시
4. 개인정보 보유부서의 사용자권한 설정 등 제반 보호장치가 잘 운영되고 있는지 확인 · 감독
5. 개인정보보호 관리실태에 대한 점검 및 지도
6. 각종 개인정보보호 관련 통계 및 자료 취합

7. 개인정보보호 관련사항에 대해 청직원 · 민원인에 공지 및 교육
8. 그 밖에 개인정보 보호를 위해 필요한 사항 등

제25조(개인정보취급자의 역할 및 책임) ① 업무상 개인정보를 처리하는 자는 처리하는 개인정보가 훼손 및 누설되지 않도록 개인정보보호지침에 따라 안전하게 취급하여야 한다.

② 직무상 알게 된 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용해서는 아니 된다.

③ 개인정보 접근 권한을 임의로 양도 및 대여하여서는 아니 된다.

제4절 개인정보 침해대응

제26조(개인정보의 유출) 개인정보의 유출이라 함은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것으로서, 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우
4. 그 밖에 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

제27조(통지시기 및 항목) ① 실제로 유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없으면 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

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

② 개인정보처리자는 제1항제2호의 경우 개인정보 유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증하여야 한다.

③ 개인정보처리자는 제1항 각 호의 조치를 취한 이후에는 정보주체에게 다음 각 호의 사실만을 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실

2. 제27조제1항의 통지항목 중 확인된 사항

제28조(통지방법) ① 정보주체에게 제27조제1항 각호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 정보주체에게 알려야 한다.

② 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제27조제1항 각호의 사항을 공개할 수 있다.

제29조(개인정보 유출신고) ① 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 5일 이내에 안전행정부장관 또는 시행령에 명시된 전문기관 중 어느 하나에 신고하여야 한다. 〈개정 2013.4.2〉

② 제1항에 따른 신고는 별지 제1호 서식에 따른 개인정보 유출신고서를 통하여 하여야 한다.

③ 전자우편, 팩스 또는 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제27조제1항의 사항을 신고한 후, 별지 제1호 서식에 따른 개인정보 유출신고서를 제출할 수 있다.

④ 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제27조제1항에 따른 통지와 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 제27조제1항 각호의 사항을 7일 이상 게재하여야 한다.

제30조(개인정보 침해신고 처리절차) ① 부서별 개인정보보호 업무담당자는 침해사고 발생 또는 신고가 접수되면 즉시 개인정보 보호책임자에게 통보하여야 한다.

② 접수된 개인정보 침해신고에 대한 상담안내는 7일 이내, 신고 조사처리는 30일 이내에 조치 완료하여야 하며, 조치 후 신고인과 안전행정부에 처리결과를 통보하여야 한다. 〈개정 2013.4.2〉

제31조(개인정보 침해사고 대응) 개인정보침해사고에 대한 일반적인 대응방법은 『통계청 정보보호 침해사고 대응지침』을 따른다.

제5절 정보주체의 권리 보장

제32조(개인정보 열람 연기 사유의 소멸) ① 법에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없다면 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 시행령에 따른 개인정보의 제3자 제공현황의 열람청구를 받은 경우, 국가안보에 긴요한 사안으로 법의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제33조(개인정보의 정정 · 삭제) ① 법에 따른 개인정보의 정정 · 삭제 요구를 받았을 때에는 정당한 사유가 없다면 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정 · 삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정 · 삭제 요구가 법에 명시된 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제34조(개인정보의 처리정지) ① 정보주체로부터 법에 따라 개인정보처리를 정지하도록 요구받은 때에는 법의 단서에 해당하지 않고 다른 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보의 처리의 일부 또는 전부를 정지하여야 한다.

② 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여는 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 별지 제2호 서식에 따른 통지서를 통하여 정보주체에게 알려야 한다.

제35조(권리행사의 방법 및 절차) 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집 시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다. 이는 시행령에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 수수료와 우송료의 정산에도 마찬가지로 적용된다.

제6절 개인정보 처리방침 작성

제36조(개인정보 처리방침의 공개) 법에 따라 개인정보 처리방침을 수립하거나 변경하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며 이 경우 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

제37조(개인정보 처리방침의 변경) 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록

변경 전 · 후를 비교하여 공개하여야 한다.

제38조(개인정보 처리방침의 작성기준 등) ① 개인정보 처리방침을 작성할 때에는 법 및 시행령에서 규정된 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 개인정보의 처리 목적에 필요한 최소한의 개인정보라는 점을 밝혀야 한다.

③ 목적에 필요한 최소한의 개인정보 이외에 개인별 맞춤서비스 등을 위하여 처리하는 개인정보의 항목이 있는 경우에는 양자를 구별하여 표시하여야 한다.

제39조(필수적 기재사항) 개인정보처리방침을 작성할 때에는 법에 따라 다음 각 호의 사항을 모두 포함하여야 한다.

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체의 권리 · 의무 및 그 행사방법에 관한 사항
6. 처리하는 개인정보의 항목
7. 개인정보의 파기에 관한 사항
8. 개인정보 보호책임자에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 시행령에 따른 개인정보의 안전성 확보조치에 관한 사항

제40조(임의적 기재사항) 제39조의 필수적 기재사항 이외에도 다음 각 호의 사항을 개인정보 처리방침에 포함할 수 있다.

1. 정보주체의 권익침해에 대한 구제방법
2. 개인정보의 열람청구를 접수 · 처리하는 부서

제3장 개인정보 안전조치

제1절 기술적 안전조치

제41조 (접근 권한의 관리) ① 개인정보처리시스템에 대한 접근권한은 업무 수행에 필요한 최소한의 범위로 개인정보취급자에 따라 차등 부여하여야 한다.

② 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 삭제하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 삭제에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

제42조 (비밀번호 관리) 개인정보취급자의 비밀번호 관리는 「통계청 정보보안 업무규정 시행세칙」을 준용한다.

제43조 (접근통제 시스템 설치 및 운영) ① 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치 · 운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다.

③ 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터만을 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

제44조 (개인정보의 암호화) ① 고유식별정보, 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 제1항에 따른 개인정보를 정보통신망을 통하여 송 · 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑤ PC에 고유식별정보가 포함된 개인정보를 저장하여 관리하는 경우해당 파일을 암호화한 후 저장하여야 한다.

제45조 (접속기록의 보관 및 위·변조방지) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하도록 하여야 한다.

② 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제46조 (보안프로그램 설치 및 운영) 개인정보처리자는 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시
2. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제47조 (물리적 접근 방지) ① 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보취급자는 개인정보가 포함된 서류, 보조저장매체 등을 안전한 이중 시건장치 캐비닛에 보관하여야 한다.

제2절 관리적 안전조치

제48조 (개인정보의 관리) ① 기관 내 부서간의 개인정보 이용 또는 조회가 필요할 경우, 법령에 근거하거나 소관업무를 수행하기 위해 필요한 최소한의 범위로 제한하여야 한다.

② 개인정보처리자는 정보주체의 동의 없이 개인정보를 수집하거나 보유목적 외 또는 보유목적에 맞더라도 권한을 넘어서는 부당한 목적으로 내부직원 등이 이용 또는 조회하지 못하도록 엄격하게 관리하여야 한다.

제49조 (개인정보 접속기록의 점검) 개인정보취급자는 개인정보처리시스템의 개인정보에 접속한 기록을 최소 6개월 이상 보관·관리하여야 하며, 접속한 기록이 위·변조 및 도난, 분실되지 않도록 접속기록을 매월 소속 부서장에게 보고하여야 한다.

제50조 (개인정보 노출사고 예방) ① 개인정보를 포함한 자료를 홈페이지 등에 게시하기 전 개인정보취급자는 반드시 상급자에게 보고 절차를 거쳐야 한다.

② 개인정보취급자의 소속 부서장은 홈페이지 등에 부주의하게 개인정보가 게재되지 않도록

감독해야 하며, 개인정보노출사고가 발생 시 즉시 해당 게시물을 삭제하는 등 초동조치 후 개인정보보호책임자에게 보고하여야 한다.

제51조 (개인정보보호 교육) ① 개인정보보호책임자는 관계기관이 주최하거나 실시하는 워크숍, 컨퍼런스 또는 개인정보보호 전문교육을 연 1회 이상 참석하여야 한다.

② 개인정보보호책임자는 개인정보취급자에 대하여 개인정보보호 관련 법률 및 제도 등 개인정보보호에 필요한 내용을 연 2회 이상 교육하여야 한다.

③ 제2항을 시행함에 있어 개인정보보호책임자는 개인정보취급자에 대한 교육을 개인정보보호 업무담당자에게 위임할 수 있다.

제52조 (보안서약서 작성) 개인정보취급자 및 부서별 개인정보보호 업무담당자는 지정됨과 동시에 개인정보보호책임자에게 개인정보보호와 관련된 별지 제3호 서식에 따른 서약서를 작성한 후 제출하여야 한다.

제4장 개인정보파일 등록 · 공개

제1절 총 칙

제53조(적용대상) 이 장은 통계청 및 소속 기관에서 보유하고 있는 개인정보파일을 적용대상으로 한다.

제54조(적용제외) 이 장은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 관하여는 적용하지 아니한다.

1. 법에 따라 적용이 제외되는 다음 각목의 개인정보파일

   가. 국가안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일

   나. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일

   다. 다른 법령에 따라 비밀로 분류된 개인정보파일

2. 법 제58조제1항에 따라서 법 적용이 제외된 「통계법」에 따라 수집되는 개인정보파일

3. CCTV 등 영상정보처리기기를 통하여 처리되는 개인영상정보파일

4. 자료 · 물품 또는 금전의 송부, 1회성 행사 수행 등의 목적만을 위하여 운용하는 경우로서 저장하거나 기록하지 않고 폐기할 목적으로 수집된 개인정보파일

제2절 개인정보파일의 등록주체와 절차

제55조(개인정보파일 등록 주체) 개인정보파일을 운용하는 개인정보 보호책임자는 그 현황을 안전행정부에 등록하여야 한다. 〈개정 2013.4.2〉

제56조(개인정보파일 등록 및 변경 신청) ① 개인정보파일 등록 신청 사항은 다음의 각호와 같다

1. 개인정보파일을 운용하는 기관의 명칭
2. 개인정보파일의 명칭
3. 개인정보파일의 운영 근거 및 목적
4. 개인정보파일에 기록되는 개인정보의 항목
5. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
6. 개인정보의 처리방법
7. 개인정보의 보유기간
8. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
9. 개인정보 처리 관련 업무를 담당하는 부서
10. 개인정보의 열람 요구를 접수 · 처리하는 부서
11. 개인정보파일의 개인정보 중 법에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
12. 법에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과

② 개인정보취급자는 개인정보파일을 새로 등록하거나, 또는 등록된 사항이 변경된 경우에는 개인정보 보호책임자에게 별지 제4호 서식에 따른 신청서를 통하여 변경을 신청하여야 한다.

제57조(개인정보파일 등록 및 변경 확인) ① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록 · 변경 사항을 검토하고 그 적정성을 판단한 후 안전행정부에 등록하여야 한다. 〈개정 2013.4.2〉

② 통계청의 각 소속기관은 개인정보 보호책임자에게 제1항에 따른 등록 · 변경 사항의 검토 및 적정성 판단을 요청한 후, 확인을 받아 안전행정부에 등록하여야 한다. 〈개정 2013.4.2〉

제58조(개인정보파일 등록 및 변경 기한) 제57조의 등록은 60일 이내에 하여야 한다.

제59조(개인정보파일의 파기) ① 개인정보파일의 보유기간 경과, 처리목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보취급자는 보유기간 경과, 처리목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, 별지 제5호 서식에 따른 개인정보파일 파기요청서에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호책임자의 승인을 받아 개인정보를 파기하여야 한다.

③ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 별지 제6호 서식에 따른 개인정보파일 파기 관리대장을 작성하여야 한다.

제60조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제59조에 따라 개인정보파일을 파기한 경우, 법에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체 없이 등록 사실을 삭제한 후 그 사실을 안전행정부에 통지한다. 〈개정 2013.4.2〉

제61조(등록 · 파기에 대한 개선권고) 개인정보 보호책임자는 제56조제1항에 따라 검토한 개인정보파일이 과다하게 운용되고 있다고 판단되는 경우에는 개선을 권고할 수 있다.

제3절 개인정보파일의 관리

제62조(개인정보파일대장 작성) ① 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

② 개인정보파일대장 작성은 제56조제2항의 신청에 따라 개인정보파일이 안전행정부에 등록되면 이루어진 것으로 간주한다. 〈개정 2013.4.2〉

제63조(개인정보파일 이용 · 제공 관리) 법에 따라 제3자가 개인정보파일의 이용 · 제공을 요청한 경우에는 각각의 이용 · 제공 가능 여부를 확인하고 별지 제7호 서식의 '개인정보 목적 외 이용 · 제공대장'에 기록하여 관리해야 한다.

제64조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.

② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의

협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 다만, 보유기간은 별표 1의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과「공공기록물 관리에 관한 법률 시행령」에 따른 기록관리기준표를 상회할 수 없다.

③ 정책고객, 홈페이지회원 등의 홍보 및 대국민서비스 목적의 외부고객 명부는 특별한 경우를 제외하고는 2년을 주기로 정보주체의 재동의 절차를 거쳐 동의한 경우에만 계속적으로 보유할 수 있다.

제65조(개인정보파일 현황 관리) 개인정보 보호책임자는 개인정보파일의 보유 · 파기현황을 주기적으로 조사하여 그 결과를 개인정보 처리방침에 포함하여 관리해야 한다.

제5장 보 칙

제66조(처리 중인 개인정보에 관한 경과조치) ① 법 시행 전에 근거법령 없이 개인정보를 수집한 경우 해당 개인정보를 보유하는 것은 적법한 처리로 본다. 다만, 이 법 시행 이후 기존의 수집 목적 범위에서 이용하는 경우를 제외하고 개인정보를 새롭게 처리하는 경우에는 법, 시행령, 시행규칙 및 이 지침에 따라야 한다.

② 법 시행 전에 법률의 근거 또는 정보주체의 동의 없이 제3자로부터 개인정보를 제공받아 목적 외의 용도로 이용하고자 할 경우 정보주체의 동의를 받아야 한다.

③ 법 시행 전에 개인정보를 수집한 경우 기존의 수집목적 범위에도 불구하고 제1항 단서 및 제2항을 준수하기 위하여 새롭게 정보주체의 동의를 받을 목적으로 법 시행 전에 수집한 개인정보를 이용할 수 있다.

제67조(준용) 이 지침에 명시되지 않은 영상정보처리기기에 관한 사항은 『통계청 영상정보처리기기 설치운영에 관한 지침』을 따른다.

부 칙

제1조(시행일) 이 예규는 발령한 날부터 시행한다.

부 칙 〈2013. 4. 2〉

제1조(시행일) 이 예규는 발령한 날부터 시행한다.

[별지 제1호 서식]

개인정보 유출신고서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책 · 조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서 · 담당자 및 연락처		**성명**	**부서**	**직위**	**연락처**
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수기관	**기관명**	**담당자명**	**연락처**

[별지 제2호 서식]

개인정보 ([ ]정정 · 삭제, [ ]처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
☐ 정정 · 삭제 ☐ 처리정지 조치 내용	
☐ 정정 · 삭제 ☐ 처리정지 조치 내용	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정 · 삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

[별지 제3호 서식]

보안 서약서(개인정보보호)

본인은 0000년 00월 00일부로 개인정보 관련 업무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 개인정보 관련 업무 중 알게 될 개인정보와 관련된 내용이 직무상 보호할 대상임을 인정한다.

2. 본인은 개인정보를 누설함이 정보주체의 권리와 이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 개인정보를 일체 누설하거나 공개하지 아니한다.

3. 본인이 개인정보를 누설하거나 관계 규정을 위반한 때에는 관련 법령에 따라 어떠한 처벌 및 불이익도 감수한다.

4. 본인은 '개인정보보호법' 및 '통계청 개인정보보호 지침'을 준수하고 개인정보 관련 업무를 성실히 수행하겠습니다.

년 월 일

서 약 자	부 서 명 :		
	직 급 :		
	연 락 처 :		
	성 명 :		(서명)
서약집행자	직 위 :		
(소속부서장)	성 명 :		(서명)

[별지 제4호 서식]

개인정보파일 ([ ]등록 [ ]변경등록) 신청서

접수번호	접수일	처리기간 7일

공공기관 명칭	주소	등록부서	전화번호

등록항목	등록정보	변경정보 및 변경사유
개인정보파일 명칭		
개인정보파일의 운영 근거 및 목적		
개인정보파일에 기록되는 개인정보의 항목		
개인정보의 처리방법		
개인정보의 보유기간		
개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자		
개인정보파일을 운용하는 공공기관의 명칭		
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		
해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서		
개인정보의 열람 요구를 접수·처리하는 부서		
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유		

「개인정보 보호법」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이 개인정보파일 ([ ]등록 [ ]변경등록)을 신청합니다.

년 월 일

[별지 제5호 서식]

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

[별지 제6호 서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

[별지 제7호 서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보 파일 명칭			
이용 또는 제공 구분	[ ]목적외 이용 [ ]제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속 성 명 전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명 소 속 전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

[별표 1호]

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

참고4

2013년 OECD 개정 개인정보보호 가이드라인

■ 개요

○ OECD 이사회는 2013년7월11일 프라이버시보호와 개인정보 국외 이전에 관한 가이드라인(개인정보보호가이드라인) 개정안을 채택함

- 이 개정안은 **1980년에 가이드라인이 배포된 이래 처음**이며, 2008년 인터넷경제의 미래를 위한 서울선언문의 지침 "변화하는 기술, 시장과 이용자 행태, 증가하는 사이버 정체성의 중요성"에 따라 가능하고자하는 장관들의 요청에 의해 개정됨

○ 개정된 가이드라인에는 **두 가지 주제**가 포함되어있음

- 위험관리에 기초한 접근법에 의해 **개인정보보호의 현실적 이행**에 초점을 둠
- 향상된 상호운용성에 기초하여 **글로벌 차원의 개인정보보호**를 짚어보는 노력이 필요하다는 점

■ 주요내용

○ 개인정보보호 가이드라인의 범위

- 공공부문 또는 민간부문에 관계없이 그 처리방법, 성질 또는 사용되는 상황으로 인하여 **프라이버시 또는 개인의 자유에 위험을 초래하는 개인정보**에 적용됨
- 본 가이드라인의 원칙들은 상호보완적이며 전체로 써 읽혀져야 함
- 국가주권, 국가보안, 공공정책에 대한 것을 포함하여 예외사항은 공지되어야 하며 가능한 최소한으로 해야 함
- 이 가이드라인은 프라이버시와 개인의 자유를 보호하기 위한 추가적인

조치에 의해 보완될 수 있는 최소한의 표준으로 간주되어야 하며, 개인정보의 국외이전에 영향을 줄 수 있음

1. 국내적용의 기본원칙

○ 수집제한의 원칙

- 개인정보의 수집에는 제한이 있어야 하고, 정보는 적법하고 공정한 방법에 의해 얻어져야 하며, **정보주체의 인지 또는 동의가 있는 것이 적절한 경우**에 수집해야 함

○ 정보 정확성의 원칙

- 개인정보는 **사용 목적과 관계가 있어야 하고** 그 목적에 필요한 한도 내에서 **정확하고, 완전하며, 최신의 것**이어야 함

○ 목적명시의 원칙

- 개인정보의 수집목적은 수집이전 및 당시에 명시되어야 하며, 개인정보의 이용은 **명시된 수집목적 또는 수집 시 목적, 목적 변경 시 명시되는 목적과 상충하지 않아야 함**

○ 이용제한의 원칙

- 개인정보는 **명시된 이외의 목적으로 공개되거나 이용가능 또는 기타사용 될 수 없음.** 단, 정보주체의 동의가 있는 경우, 법률에 의해 허가된 경우에는 가능함

○ 안전성 확보의 원칙

- 개인정보는 손실 또는 권한 없는 접근, 파괴, 사용, 수정 또는 공개에 대한 적절한 **안전조치에 의해 보호되어야 함**

○ 공개의 원칙

- 개인정보와 관련하여 개발, 실행, 정책에 대한 전반적인 공개방침이 있어야 하고, 그 방법은 정보관리자의 신원 및 주소를 비롯하여 개인정보의 존재와 성질, 정보의 이용목적을 용이하게 확인할 수 있는 것이어야 함

○ 개인 참여의 원칙

- 개인들은 정보관리자로부터 또는 기타의 방법으로 **정보 관리자가 자신들에 대한 정보를 보유하고 있는지에 대해 확인할 권리**를 가짐
- 자신에 관한 정보와 통신할 수 있는 권리(적절한 시간 내에 유료라면 과도하지 않은 비용으로, 적절한 방법으로, 개인들이 쉽게 알 수 있는 형식으로)
- 위의 2가지 요청이 거부된 경우, 그 사유를 알고 이의를 제기할 수 있는 권리
- 자신의 정보와 관련된 정보에 이의를 제기하고 이의제기가 수락된 경우, 그 정보를 삭제, 정정, 완성, 수정할 수 있는 권리

○ 책임의 원칙

- 정보 관리자는 상기원칙들을 실행하기 위한 조치를 따라야하는 책임이 있음

2. 책임이행

○ 정보 관리자는 다음과 같은 **개인정보보호 관리프로그램이 준비**되어 있어야 함

- 관리 하에 있는 모든 개인정보에 대해 이 가이드라인을 실행함
- 자신의 조직의 구조, 규모, 용량, 민감도에 맞게 만들어야 함
- 프라이버시 위험평가에 기반한 적절한 보호조치를 제공해야 함
- 거버넌스 구조에 통합되고 **내부 감시 메커니즘**을 설립해야 함
- 사고 및 문의에 대응하기 위한 계획을 포함해야 함

- **지속적인 모니터링과 정기적인 평가**를 통해 업데이트되어야 함

○ 개인정보보호 관리프로그램의 적절함을 입증할 준비가 되어 있어야 함

○ 개인정보에 영향을 주는 중대한 보안 유출이 있을 때 개인정보보호 집행기관이나 다른 관련 기관들에 적절한 통지를 해야 함

- 정보 관리자는 영향을 받은 정보주체에게 통지해야 함

3. 국내 적용의 기본원칙 : 자유로운 이동과 합법적 제한

○ 정보 관리자는 데이터의 위치에 상관없이 자신이 관리하는 개인정보에 대해 책임이 있음

○ 회원국은 다음과 같은 경우 개인정보 국외이전 제한을 삼가야 함

- 다른 나라가 이 가이드라인을 대체로 준수할 경우

- 효과적인 집행 메커니즘과 정보 관리자로부터 이 가이드라인과 일관성 있는 지속적인 수준의 보호를 보장하기 위한 적절한 조치 등의 충분한 보호조치가 존재할 경우

○ 개인정보의 국외이전에 대한 어떠한 제한도 존재하는 위험에 비례해야 하며, 데이터의 민감도와 처리에 대한 목적과 사용되는 상황을 고려하여야 함

4. 국내이행

○ 이 가이드라인을 이행하기 위해 회원국들은

- 정부기관간의 통합된 접근법을 반영할 수 있는 국가 개인정보보호전략을 개발해야 함

- 프라이버시를 보호하는 법을 채택해야 함
- 권력을 효과적으로 행사하고, 객관적이며 공정하고 일관된 기준으로 의사결정을 할 수 있도록 거버넌스, 자원, 기술적 전문지식을 갖춘 개인정보보호 집행기관을 설립하고 유지해야 함
- 행동강령의 형태 또는 다른 형태로 자기규제를 장려하고 지원해야 함
- 개인이 그들의 권리를 행사할 수 있는 적절한 방법을 제공해야 함
- 개인정보보호법을 준수하지 못할 경우를 위해 적절한 제재 및 구제수단을 마련해야 함
- 교육과 인식제고, 기술발달, 개인정보보호를 위한 기술조치의 촉진을 포함한 보완조치의 채택을 고려해야 함
- 정보관리자이외의 행위자의 역할을 개별역할에 적합하게 고려해야 함
- 정보주체에 대한 불공정한 차별이 없도록 보장할 것

5. 국제협력과 상호 호환성

○ 회원국은 특히 개인정보보호 집행기관사이에서의 정보공유를 강화함으로써, 국경 간 개인정보보호법 집행협력을 촉진하기 위해 적절한 조치를 해야 함

○ 회원국은 이 가이드라인에 실질적인 효과를 주는 개인정보보호 프레임워크에 상호운용성을 촉진하는 국제협정의 개발을 장려하고 지원해야 함

○ 회원국은 프라이버시와 개인정보의 국외이전과 관련한 정책결정 프로세스에 대해 알리기 위해 **국제적으로 비교가 가능한 지표의 개발을 장려**해야 함

○ 회원국은 이 가이드라인에 대한 세부적인 준수사항을 공개해야 함

행정자료를 이용한
국가통계 작성 표준편람(II)

- 개인정보 보호편 -

| 발 행 | 2014년 9월
| 발 행 인 | 통계청장 박형수
| 편 집 인 | 행정통계과장 송성헌
| 기 획 | 최인범, 김언성, 김가영, 이정수, 이명호, 송호만
| 발 행 처 | 통계청
| 주 소 | 대전광역시 서구 청사로 189 정부대전청사(우302-701)
| 문의사항 | 042) 481-3741, 3742

| 디자인 · 인쇄 | 나래기획 042) 226-2568

발간등록번호 11-1240000-000584-01
ISBN 978-89-5801-283-2 93310