디지털로 여는 좋은 세상

2022-8호

D.gov

해외동향 법·제도

NIA

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY

CONTENTS

1 행정의 디지털화

콜롬비아 - '행정절차의 디지털화 및 자동화에 대한 온라인 완료 조건 및 지침' 시행령 마련 _ 4
스위스 - 디지털 행정에 관한 공법 프레임워크 협약 채택 _ 8

2 디지털 신원 인증

핀란드 - 디지털 신원법 초안 마련 _ 13
모나코 - 디지털 신원 인증법 제정 _ 25
뉴질랜드 - 디지털 ID 신뢰 프레임워크 법안 제안_ 30

3 자동화된 의사결정

캐나다 - 자동화된 의사결정에 대한 지침 도입 _ 33

「**D.gov 해외동향 법·제도**」는 정부의 디지털 전환을 위한 다양한 해외 법·제도 분석을 통해 입법 방향을 모색하기 위해 한국지능정보사회진흥원에서 기획발간하는 보고서입니다.

본 보고서의 내용은 한국지능정보사회진흥원의 공식 견해와 다를 수 있으며, 본 보고서의 내용에 대한 문의 및 제안은 아래 연락처로 해 주시기 바랍니다.

■ 발 행 처: 한국지능정보사회진흥원
■ 작　　성: 한국지능정보사회진흥원 디지털정부본부 디지털정부기획팀
　　- 김희진 주임(alice@nia.or.kr)
■ 기　　획: 정준원 디지털정부본부장, 박선주 디지털정부기획팀장
■ 보고서 온라인 서비스: www.nia.or.kr, egov.nia.or.kr

행정의 디지털화 1

콜롬비아, '행정절차의 디지털화 및 자동화에 대한 온라인 완료 조건 및 지침' 시행령 마련

Ⅰ 개요

○ 콜롬비아 정보통신부(MINTIC)는 디지털 수단을 통해 행정관리 및 시민과의 상호작용을 개선하는 '행정절차의 디지털화 및 자동화에 대한 온라인 완료 조건 및 지침'(Decreto 088 de 2022)의 시행령을 공식화(22.1.24.)[1)]

- '정보통신 기술 부문 단독 규제(2015 법률1078)'* 법령 제2권 2부에 제20장를 추가하여 디지털화, 자동화 및 온라인 상에서의 실행을 위한 개념, 지침, 기한 및 조건을 설정

* Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones(decreto 1078 de 2015) : 정보사회와 정보통신 기술 조직에 대한 원칙과 개념을 정의한 콜롬비아 단일 법령

〈 참고: 디지털화와 자동화의 개념 구분 〉

디지털화	자동화
가상으로 수행되더라도 완료를 위해 내부 프로세스와 관련된 일종의 인간 개입이 필요한 절차	프로세스 중에 사람의 개입이나 지원 없이 프로세스가 자율적으로 수행될 수 있도록 하는 데 필요한 시스템 및 기술 리소스의 적응 또는 구현

〈 시행령의 구성 〉

제1조 목적	제7조 사전 준비행위
제2조 적용분야	제8조 예외조항
제3조 정의	제9조 협조의무
제4조 절차의 디지털화 및 자동화에 대한 지침(부록1)	제10조 전자문서 관리, 보안 및 개인정보 보호
제5조 디지털정부 정책의 통합과 절차 합리화	제11조 비용
제6조 일반 조항	

1) https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en

Ⅱ 주요 내용

❍ 본 시행령은 모든 공공기관, 개인에 적용되며 ICT 사용을 통해 행정관리 및 시민과의 상호 작용을 개선하는 것을 목표로 함

- 해당 시행령을 통해 공공서비스의 품질을 제고하고 국가 디지털 전환 비용을 절감하고 프로세스 효율을 개선할 것으로 기대

- 콜롬비아 정보통신기술부는 국민들의 디지털 공공서비스 접근이 평등하게 이루어지도록 공무원 인력 확충과 미디어에 대한 접근을 보장하는 것을 기본원칙으로 명시

- 부록은 아키텍쳐 프레임워크에 명시된 지침과 표준, 보안 및 프라이버시의 모델, 디지털 시민 서비스 모델 절차의 합리화 정책 같은 방법론적 내용으로 구성

〈 시행령에 등장하는 주요 정의 〉

자동화	과거에는 사람이 수행하였으나 현재는 기계에 의해 자율적으로 실행되는 절차를 포함하는 일련의 작업을 실행하고 내부를 관리하는 시스템 역량을 의미
디지털화	당국의 절차(등록, 처리, 저장, 상담, 접근 및 데이터 사용)의 내부 관리와 관련된 작업 또는 절차를 개발하기 위해 사람이 개입하여 디지털 미디어를 사용하는 것을 의미
비물질화	처리 절차의 결과물로서 디지털 또는 전자적인 형식으로 제공되는 물리적 문서, 증명서, 확인서, 공식 증명서 또는 신분증의 처리를 의미하며, 개인의 사실적 또는 법적 상황과 관련하여 발행
전자 도장	전자적으로 발급 지급, 첨부 또는 취소되는 문서를 의미하며, 제공된 서비스에 대한 지불 또는 발생한 세금의 납부, 조세에 관한 규정의 이행을 증명하는 서류
상호 운용성	시민 기업 및 기타 기관들에게 디지털 서비스 제공을 촉진할 목적으로 조직이 비즈니스 프레임 워크 내에서 정보와 지식을 교환하여 상호 유익한 목표를 향해 상호작용할 수 있는 역량을 의미
공공 등록	자연인 또는 법인이 법적 의무에 따라 권한이나 의무에 대한 법적 효력을 발생시키는 당국 앞에서 사실, 행위 또는 법적 상황 등에 대하여 직접 혹은 가상으로 등록, 주석을 달거나 인증하는 행위를 의미

❍ 모든 기관은 중앙부처, 지자체 여부, 절차의 수, 제도적 성과, 요구 수준 및 절차적 복잡성, 기술의 진화 및 특성, 사회경제적 특성에 따라 블록으로 분류

- 국가기관(136개), 기타기관(3,088개)는 블록별로 2022.1.31.까지 계획을 작성하고 기한(최대 2037년) 안에 공공서비스 절차의 디지털화 및 자동화 계획을 수행할 예정

- 가장 시급히 디지털화·자동화가 진행되어야 하는 블록1은 연간 요청 건수가 많고 국민들에게 큰 영향을 끼치는 공공서비스로 행정부처, 연구소, 경제협회, 공공시설 등이 해당

〈 예시: 중앙부처의 절차 자동화 기한 ('22.1.24.시행일 기준) 〉

기관 그룹	가장 높은 순위	중간 순위	가장 낮은 순위
	블록1(절차의 30%)	블록1+2(절차의 60%)	블록1+2+3(절차의 100%)
국가 행정 부서, 부처, 산업 및 상업 기업, 혼합 경제협회, 과학 기술 연구소	22개월 (~2023년 10월)	39개월 (~2025년 3월)	57개월 (~2026년 9월)
특별 행정 기관, 교육감, 특수 성격의 국가 기관, 공공 시설, 공공 서비스 회사	23개월 (~2023년 11월)	40개월 (~2025년 4월)	58개월 (~2026년 10월)
국영 사회적 기업, 특수 법적 성격의 기관, 행정부의 기타 기관	37개월 (~2025년 1월)	62개월 (~2027년 2월)	85개월 (~2029년 1월)

❍ 완전히 디지털화되거나 자동화될 수 없는 절차인 경우에는 서비스의 성격상 허용되는 경우에 한정하여 기관 간 상호운용성을 검토하여 타 기관으로 절차를 변환하고 이동

- 특성상 온라인으로 수행할 수 없는 절차는 디지털화와 자동화의 의무를 준수한 것으로 간주하며 수행해야 하는 모든 단계는 온라인 상에서 확인 가능

❍ 또한 행정절차의 디지털화 및 자동화 프로세스에서의 문서 관리 보안 및 프라이버시를 위해 파일 전자문서 처리시스템을 통해 전자문서를 사용

- 전자 문서파일은 시민 폴더 서비스(개인화된 공공서비스 접근 창구)와 연계되며 해당 조치는 개인정보 보호 규정을 준수하여 진행되어야 함을 명시

Ⅲ 시사점

❍ 본 시행령을 통해 콜롬비아는 세분화된 업무 특성을 바탕으로 국민이 체감할 수 있도록 디지털화·자동화의 속도를 달리해서 기관별로 추진하고 이를 명문화

- 콜롬비아는 디지털화와 자동화의 개념을 세분화하였을 뿐 아니라 디지털화가 조속히 진행되어야 하는 업무의 우선순위를 매기고 기한 한에 추진해야 함을 명시

- 행정업무의 특성에 따라 완전히 디지털화와 자동화가 될 수 없는 경우까지 상정한 예외 조항까지 두어 공무원들의 업무 추진에 실효성을 추가함

❍ 국내에서도 기존의 디지털화가 이루어지지 않은 업무의 절차의 양과 질, 기술의 적용 가능성 등에 따라 업무 진행을 세분화하여 디지털화의 완급 조절이 필요

- 중앙부처와 지자체의 '오프라인' 업무와 '오프라인+디지털' 병행 업무 특성을 면밀히 고려하여 디지털화가 용이한 사업에 대한 기준에 따라 디지털화 필요

❍ 국내에서는 디지털화가 별도 입법 없이 추진되어 온 경향이 있어 국민적 관심을 고조하고 행정의 디지털화라는 입법목적의 원활한 달성을 위한 한시법 제정 고려도 필요

- 기존에는 전자정부법 제5조에 따라 전자정부기본계획과 제5조의2 기관별 계획 수립 및 점검을 근거로 지속적으로 전자정부 계획 수립과 추진을 의무화 함

〈 행정의 디지털화 관련 국내 정책 〉

발표일	정책명	주요내용
'19.10.29.	디지털 정부혁신 추진계획	모바일 신분증이 도입되고, 전자증명서 대폭 확대
'20.6.23.	포스트 코로나 시대의 디지털 정부혁신 발전계획	코로나19 위기를 디지털 정부혁신의 가속화의 계기로 삼아 비대면 수요에 부응하고 디지털 뉴딜사업 수행
'21.6.23.	제2차 전자정부 기본계획	지능형 서비스 혁신, 데이터 행정 강화, 디지털 기반확충 등

- 그러나 정부 효율의 극적향상을 위해서는 지속적인 디지털화 노력과 더불어 강력한 정부의 의지를 담은 입법을 바탕으로 전부처의 획기적 대전환도 수반되어야 함

행정의 디지털화 2

스위스, '디지털 행정에 관한 공법 프레임워크 협약' 채택

Ⅰ 개요

❍ 스위스 정부의 디지털화를 위해 강력한 통제력과 추진체계를 가진 "디지털 스위스 관리 프로젝트"의 단계적 추진에 대한 공감대 형성

- 기존의 전자정부의 방식으로는 연방정부와 주 정부마다 다른 방식으로 디지털 혁신을 추진하여, 주 정부의 디지털 역량에 따라 혁신의 속도와 발전단계가 달리 진행

- 또한 데이터 관리의 일회성 원칙 또는 관리 프로세스의 광범위한 자동화와 같은 관리활동에 대한 새로운 요구가 증가

〈 참고 : 디지털 스위스 관리 프로젝트 〉

- 기존에는 스위스의 디지털 행정을 구축하기 위해 제3자 조직인 스위스 전자정부에 의해 조정될 공동전자정부 전략을 정의하고 기본적인 전자정부 서비스를 구축해왔음(2008.~2021.)
- 연방, 주, 지방자치단체 및 도시는 디지털 행정의 관리를 위한 협력을 강화하기 위한 디지털 스위스 관리 프로젝트를 추진(2020.4.)
- 디지털 스위스 관리 프로젝트를 통해 새로운 공동 조직을 만들고 기존의 인적 및 재정적 자원을 재결합하여 효과적으로 사용할 예정

- 디지털 스위스 관리 프로젝트를 담당할 수 있는 새로운 조직으로 "디지털 스위스 관리조직(Digitale Verwaltung Schweiz;DVS)"를 제시

❍ 스위스 주 정부 총회는 디지털 스위스 관리 조직(DVS)과 협력의 근거를 규정한 "디지털 행정에 관한 공법 프레임워크 협약*"을 승인(2021.12.17.)[2)]

* Öffentlich-rechtliche Rahmenvereinbarung über die Digitale Verwaltung Schweiz

- 협약의 기본 초안은 2021년 3월에 제출되었고, 본 승인에 따라 2022.1.1. 발효되어 2023.12.31.까지 유효하며 해지되지 않는 이상 유효기간이 1년씩 연장될 예정

---

2) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694&qid=1658714231012

Ⅱ 주요 내용

○ 스위스 디지털 전환을 위한 대원칙을 천명하고, 협력 규제 방식의 방안으로 디지털 스위스 관리조직의 법적 근거를 마련

- 스위스 행정부는 입법을 통해 디지털 스위스 관리조직이 디지털 혁신을 담당하게 됨을 명시
- 디지털 스위스 관리조직은 정치 플랫폼과 표준을 개발하며 스위스 전자정부 및 스위스 정보기술 컨퍼런스 운영을 담당하여 행정의 디지털 혁신을 위한 의견 수렴 역할을 수행

○ 디지털 스위스 관리조직이 디지털화를 위해 전략적 제어 및 조정을 설계할 수 있도록 조직의 역할, 의무, 구성, 운영방식, 자금조달 방식 등 구체적인 조직 운영 전반에 대해 규정

- 디지털 스위스 관리조직은 전략설정, E-ID 개발 지원, 신기술 보급 지원 및 표준화, 공공 ICT 커뮤니티 및 네트워킹 지원, 디지털 행정 현황 모니터링 등 명문화
- 역할 수행을 위해 내부적으로 구속력이 있는 권장 사항을 만들 수 있으며 스위스의 전자정부 전문가 그룹과 협력할 수 있다는 세부 사항도 조문화함

〈 디지털 스위스 관리 조직 조직도 〉

출처 : https://www.digitale-verwaltung-schweiz.ch/ueber-uns/digitale-verwaltung-schweiz/die-digitale-verwaltung-schweiz

〈 공법 프레임워크 협약의 조문 구성 〉

1. 주제 및 범위		
2. 원칙		
3. 개별 계약에 따른 후원, 파트너 및 커뮤니티	3.1 후원	
	3.2 파트너	
	3.3 개별 계약 커뮤니티	
4. 이행의무	4.1 작업완료 원칙	
	4.2 작업	
	4.3 전략	
	4.4 실행계획	
	4.5 모니터링 및 제어	
	4.6 평가	
5. 조직	5.1 개요	
	5.2 정치지도부	5.2.1 작업
		5.2.2 구성
		5.2.3 헌법, 의장 및 운영 방식
	5.3 운영관리 기관	5.3.1 작업
		5.3.2 구성
		5.3.3 헌법, 의장 및 운영 방식
	5.4 대의원 회의	5.4.1 작업
		5.4.2 구성
		5.4.3 헌법, 의장 및 운영 방식
	5.5 스위스의 디지털 행정을 위한 연맹 및 주의 커미셔너	5.5.1 작업
		5.5.2 임명 및 조직상태
	5.6 사무실	5.6.1 작업
		5.6.2 조직
6. 작업 그룹, 성과 관리 및 커뮤니케이션	6.1 작업 그룹	6.1.1 약속 및 작업
		6.1.2 작업반의 구성 및 작업방법
	6.2 성과관리자	6.2.1 서비스 제공자의 역할
		6.2.2 선정 및 수행계약
	6.3 커뮤니케이션 채널	6.3.1 목적과 형태
		6.3.2 구성, 소집 및 기능

7. 자금 조달	7.1 재무 계획 및 통제	
	7.2 기본 및 추가 자금 조달	
	7.3 프로젝트 및 서비스의 개별 자금 조달	
	7.4 미사용 자금 이체 ; 손실보상	
	7.5 추가 자금	
8. 보고 및 감독	8.1 정치적 감독	
	8.2 재정 감독	
9. 준거법 및 핵임		
10. 취소 정책		
11. 최종 규정	11.1 과도기 조항	
	11.2 유효일자 및 유효기간	

Ⅲ 시사점

❍ 스위스는 본 공법 프레임워크 협약을 통해서 연방정부와 주 정부를 아우르는 거버넌스를 마련하여 한정된 시간과 자원하에서 체계적으로 디지털화를 추진

- 연방정부와 주정부의 커뮤니케이션 창구를 '디지털 스위스 관리 조직'으로 일원화하고 조직의 역할, 구성, 예산, 보고 감독 규정을 법률화

- 데이터 관리의 일회성 원칙, 관리 프로세스의 자동화 등의 디지털화 목표를 달성할 예정이며 추가적으로는 정치적 플랫폼 구축을 추진할 계획

❍ 국내에도 행정안전부 중심으로 정례적인 중앙부처와 지자체 간 디지털 협력체를 마련하고 법률에 명시하여 효율적이고 합리적인 디지털 행정 구현의 노력 필요

- 오늘날의 행정 서비스는 오프라인의 과정을 온라인으로 옮기는 단순 전자화나 전자화에 효율을 가미한 디지털화의 수준을 뛰어넘어 유기적 업무 설계가 요구됨

- 최근 국내에서도 중앙부처에서부터 시작된 디지털화가 지자체 오프라인 업무에 상호영향을 주면서 부처와 지자체 간 협력 사례가 증가

〈 참고 : 중앙부처의 디지털화가 지자체의 오프라인 업무를 변화시킨 사례 〉

[방문에 의한 맞춤 공공서비스 안내]

- 수혜적 공공서비스에 대한 정보를 오프라인에서 온라인으로 변환하여 제공하던 시대와는 달리, 보조금24로 개인별 맞춤형 공공서비스 안내가 가능해짐
- 복지 사각지대 해소 차원에서 개인에게 디지털화된 맞춤형 공공서비스 정보를 적극 제공하기 위해 해당 법적 근거를 마련하고 오프라인에서의 별도 방문 절차를 신설

수혜적 공공서비스 목록관리 및 맞춤 안내에 관한 규정: 제16조의2(방문에 의한 맞춤 안내 등)

① 지방자치단체의 장은 고령, 장애, 생계활동 등으로 인해 전자정부 포털 또는 시·군·구, 읍·면·동 방문을 통해 제16조제1항에 따른 안내를 받거나 신청을 하기 어려운 주민에 대해서는 가정을 방문하여 맞춤 안내 및 신청을 위한 지원을 제공할 수 있다.

② 제1항에 따른 지원을 위하여 필요한 기준 및 방법에 관하여는 제16조 및 제17조의 규정을 준용한다.

- 중앙부처가 디지털화를 추진하고 지자체가 수행하는 하향적 디지털화를 탈피하고 협력체에서의 교감을 통해 실효적인 디지털 행정업무 수행이 이루어질 수 있도록 노력 필요

디지털 신원인증 1 핀란드, '디지털 신원법' 초안 마련

Ⅰ 개요

❍ 2020년 핀란드 재무부는 디지털 신원 활용 및 개발 프로젝트를 수립하고, 인구정보 시스템에 등록된 인원을 대상으로 한 신원증명 제공 솔루션 생산·구현의 필요성을 확인

- EU국가들은 유럽 이사회로부터 eIDAS(전자본인인증 및 신원 확인 규정)를 준수하여 보안 수준이 강화되고 최소한의 신뢰성을 가진 디지털 ID 마련에 대한 강한 요구에 직면

〈 참고 : 기타 디지털 신원활용 및 개발 프로젝트 구현 배경 〉

주요 내용
1. 전자적 신원확인의 필요성 대두 프로젝트 당시의 신원확인 수단으로는 은행에서 제공하는 은행 ID, 통신사의 모바일 증명서, 경찰청에서 발급한 신분증, 디지털 인구정보국이 발급한 시민 증명서가 존재했으나 안정성이 매우 높은 강한 정도의 안전한 전자적 신원확인 방법에 대한 수요 증가
2. 신뢰성이 담보된 전자적 신원확인 서비스 확대 전망 민간 사업자 중심으로 전자적 신원확인 서비스가 제공되었으나, 공신력 있는 전자적 신원 확인 서비스의 수요도 꾸준하므로 타임 스탬프와 개인정보의 무결성이 확보된 공공의 전자적 신원 확인 서비스의 활용 증가 예상
3. 신분증 및 여권의 발급 간소화 및 보안 강화의 요구 증가 기존에는 전자적 신분증(핀란드 시민증, 외국인증, 미성년자 시민증)은 현장 발급만 가능해서 번거로움이 있었고, 신분증에 생체정보(안면인식정보, 지문 등)가 포함되면서 보안에 대한 우려 증가
4. 디지털 인구정보국의 인증업무의 신설 인구정보시스템에 개인정보를 최초로 저장하는 경우에 디지털 ID 발급에 필요한 고유 식별 정보를 제공받아 저장하는 업무를 수행
5. 공공행정을 위한 전자적 신원확인 필요성 확인 - 디지털서비스법의 제2장 제5절에 따르면 핀란드는 모든사람에게 디지털 서비스 또는 기타 디지털 데이터 전송 방법을 사용하여 비즈니스 요구와 관련된 전자문서 전달 기회를 제공해야 함 - 또한 강한 전자적 신원확인을 통해 건강정보, 개인정보, 사회복지정보, 학생복지정보, 영업 비밀에 관한 정보를 처리할 필요성이 증가

❍ 해당 프로젝트는 디지털 신원 문서 및 해외 디지털 거래 도구의 생산 및 사용을 가능하게 하고 디지털 ID카드 및 모바일 애플리케이션을 지원하는 것을 목표로 함

- 모바일 애플리케이션으로 구현된 디지털 신분증(디지털ID 카드)은 경찰과 디지털 인구정보국이 보유한 국민의 개인정보를 제시하며, 디지털 거래에 활용될 예정
- 디지털 ID카드는 여권 및 ID카드와 같은 신분 문서 역할과 강력한 전자 식별의 기능을 포함
- 모바일로 구현된 디지털 신분증을 사용하기를 원하지 않거나 사용할 수 없는 사람들을 위한 대체 식별 수단을 사전에 마련하였다는 점이 특징적

❍ 핀란드 재무부는 디지털 신원법 정부안을 마련하고 이에 대한 후속 대응으로 전자신분증이나 강력한 전자식별 및 전자신탁서비스에 관한 법률* 등 타법 개정안까지 함께 제안(2022.02.21.)

* Hallituksen esitys eduskunnalle digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi

- 프로젝트의 디지털 신분증(디지털 ID) 서비스 및 발행은 2023년 6월 30일까지 진행될 예정이며, 디지털신분증에 관한 솔루션 구현을 위해 재무부는 자문을 거쳐 총 8개 법의 개정안을 마련
- 개정안 초안은 2022년 4월 8일 입법 의견 수렴을 완료했으며, 법안의 내용을 보완하여 핀란드 전역에서 2023년 일 시행될 예정

〈 디지털 신원활용 및 개발 프로젝트 구현을 위해 개정이 필요한 법률 〉

법률명
1. 전자인구정보원의 디지털신원인증 서비스에 관한 법률
2. 디지털 신분증에 관한 법률
3. 강력한 전자식별 및 전자신탁서비스에 관한 법률
4. 경찰 업무에서의 개인정보 처리에 관한 법률
5. 신분증에 관한 법률
6. 여권법
7. 전자인구정보원의 인구정보시스템 및 인증업무에 관한 법률
8. 행정부의 공동 전자거래 지원 서비스에 관한 법률

Ⅱ 주요 내용

❍ 디지털 인구정보국이 디지털 신분증을 발급하는 역할을 수행하고, 디지털 신분증을 토대로 디지털 신분증 서비스를 제공하는 일련의 과정을 개정사항에 포함

* Hallituksen esitys eduskunnalle digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi

❍ **(디지털 신분증에 관한 법률)** 디지털 신분증의 정의, 요건, 규격, 포함된 정보, 수명주기, 활용에 대한 부분을 법으로 명시하여 디지털 신분증을 활용한 디지털 신원증명 서비스와 분리한 것이 특징

〈 디지털 신분증에 관한 법률 〉

제1장 일반조항

제1조 (목적) 이 법은 핀란드에 거주하는 핀란드 국민 및 외국인에게 발급되는 디지털 신원 증명서에 대한 내용을 법률로 정한다.

제2조 (정의)

1) 검증된 정보 : 국가에 의해 전자적으로 검증된 개인정보를 의미한다.
2) 신뢰당사자 : 디지털 신분증 소지자에게 자신의 신원 또는 검증된 정보를 보여주고 정보의 정확성을 확인해야 하는 자연인 또는 법인을 의미한다.
3) 디지털 신분증 소지자 : 핀란드의 디지털 신분증을 소지한 자를 의미한다.
4) 기술 플랫폼 : 디지털 신분증 소지자의 모바일 단말 장치를 의미한다.
5) 방문 거래 : 디지털 신분증 소지자의 신원 또는 검증된 정보가 신뢰 당사자에게 표시되는 거래 상황을 의미한다.
6) 신원 증명: 핵심 신원 증명과 함께 디지털 인구정보국의 디지털 신원 서비스에 관한 법률 제10조에서 언급된 증명을 의미한다.

제3조 (디지털 신분증) 제1항 디지털 신분증은 전자거래 및 대면 거래를 위해 디지털 인구정보국에서 발급한 신원 및 검증된 정보가 포함된 신분증을 의미한다.
제2항 디지털 신분증은 기술 플랫폼에서 사용될 수 있도록 제공되며, 기술 플랫폼은 디지털 신원 서비스에 관한 법률 제4조에 따라 구현된 디지털 신원 정보시스템을 의미한다.

제4조 (디지털 신분증의 등록) 경찰은 디지털 신분증을 생성, 제공할 목적으로 디지털 신분증, 소유자의 유효성에 대한 레지스터를 유지관리해야 한다.

제2장 디지털 신분증에 포함된 정보 및 수명 주기

제5조 (디지털 신분증에 포함된 정보) 경찰은 개인카드법(663/2016) 제31조에 언급된 개인 카드 등록부 또는 여권법(671/2006) 제29조에 언급된 여권 등록부에 포함된 개인정보 사본을 디지털 신분증

소지자에게 전달한다. 디지털 신분증 소지자에게는 다음과 같은 개인정보가 제공된다.
(1) 이름 2) 성 3) 생년월일 4) 그 사람의 성별에 관한 정보 5) 핀란드 시민에 대한 정보 6) 개인 식별 번호 또는 기타 국가 식별 번호 7) 여권 또는 신분증 등록부에 저장된 얼굴 이미지 8) 유효한 핀란드 여권 또는 신분증의 유효기간
디지털 인구정보국에서는 디지털 신분증 소지자에게 생년월일을 기준으로 한 연령 증명서를 교부한다. 디지털 신분증 소지자에게 개인정보의 사본을 제출하기 전에 정보를 확인할 의무가 있으므로 경찰은 인증서의 유효성을 확인하기 위하여 정보가 최신인지 확인할 수 있다. 경찰은 정보가 디지털 신분증 소지자에게 제공된 후 개인에게 제공된 검증된 정보를 처리할 권리가 없다.
디지털 신분증을 사용하기 위한 조건은 디지털 신분증에 포함된 정보가 항상 최신 상태이며, 전단에서 언급된 정보와 일치해야 한다.

제6조 (디지털 신분증의 사용) 디지털 신분증은 유효한 핀란드 여권 또는 신분증을 소지한 사람이 사용할 수 있다. 시행을 위해서 경찰은 디지털 인구정보국에서 발급한 핵심 신원 증명서를 자연인에게 첨부해야 한다. 개인은 강력한 디지털 식별 및 디지털 신뢰 서비스에 관한 법률(617/2009)의 제2조나 제1조에서 언급된 강력한 디지털 신분증을 사용하거나 권한 있는 여권 또는 디지털 신분증 기관과 거래하여 디지털 신분증을 사용할 수 있다. 후자의 경우에도 유효한 여권이나 신분증의 기술적인 부분에 있는 정보를 원격으로 읽어야 하며 강력한 디지털 식별을 통해 얻은 정보와 일치해야 한다.

제7조 (디지털 신분증의 유효성) 디지털 신분증은 핵심 신원증명을 포함해야 효력이 있다. 핵심 신원 증명의 유효성은 디지털 및 인구정보국의 디지털 신원 서비스에 관한 법률 섹션 12에 규정되어 있다.

제8조 (디지털 신분증의 취소) 디지털 신분증은 당사자의 요청에 의해서만 취소될 수 있다. 경찰은 명백한 이유로 기본 신분문서가 취소되거나 디지털 신분증 소지자가 아닌 다른 사람이 사용하는 경우 디지털 신분증을 취소할 수 있다.

제3장 활용

제9조 (디지털 신분증의 제시) 디지털 신분증 소지자는 신뢰기관에 보여줄 정보를 표시할 수 있다. 정보를 전자적으로 공유할 때는 경찰이 만든 관련 정보 및 중앙집중식 신분증의 보증 수준은 항상 공개된다.

제10조 (대면 방문 시 확인된 정보 표시) 대면 방문에서 디지털 신분증 소지자는 신뢰 당사자에게 보여주고 싶은 정보만 선택해서 보여줄 수 있다. 그러나 방문 시에는 반드시 얼굴을 보여야 한다. 필요한 경우 정보를 수신하는 신뢰당사자는 디지털 신원에 관한 법률 제13조제1항에 언급된 핵심 신원증명 등록부에서 디지털 신분증 소지자의 핵심 신원 증명 유효성을 확인할 권리가 있다. 또한 경찰은 디지털 인구정보국이 관리하는 디지털 신분정보 시스템에서 전자신분증의 정보를 확인할 권리가 있다.

제11조 (디지털 신분증 소지자의 책임) 디지털 신분증 소지자는 디지털 신분증을 주의해서 보관해야 한다. 디지털 신분증을 관리해야 하는 디지털 신분증 소지자의 의무는 디지털 신분증을 사용할 때 시작된다. 디지털 신분증 소지자는 타인에게 디지털 신분증을 양도할 수 없다. 디지털 신분증 소지자는 문제를 발견하는 즉시 디지털 신분증의 분실, 무단 소유 또는 무단 사용에 대해 디지털 인구정보국에 알려야

한다. 디지털 인구정보국은 언제든지 보고할 수 있는 가능성을 제공해야 한다. 디지털 인구정보국은 고지를 받은 후 즉시 디지털 신분증의 기본 신분 증명을 취소하거나 사용을 금지하여야 한다.

❍ **(디지털 신원인증 서비스에 관한 법률)** 모바일 애플리케이션으로 구현된 디지털 신분증(디지털ID 카드)은 경찰과 디지털 인구정보국이 보유한 국민의 개인정보를 제시하며, 디지털 거래에 활용될 예정

- 디지털 신원정보 시스템의 필수사항, 핵심 신원증명의 요건, 외국인의 디지털 ID 서비스 사용에 대한 내용까지 디지털 신원인증 서비스를 중심으로 한 법률을 제정

〈 디지털 신원인증 서비스에 관한 법률 〉

제1장 일반조항

제1조 (적용범위) 이 법은 디지털 인구정보국이 디지털 ID를 생성하고, 서비스를 제공하는데 필요한 내용을 규정한다.

제2조 (정의)

1) 디지털ID 서비스 : 디지털 ID 정보시스템, 핵심 신원증명, 외국인 디지털 거래 도구, 디지털 신원 관리 서비스 및 판독기 인터페이스 및 확인 응용프로그램을 의미
2) 핵심 신원 : 일반적으로 신원을 식별할 수 있는 인구 정보시템에 등록되 개인정보의 총체로 디지털 인구정보국의 인증 서비스에 관한 법률(661/2009)제13조 제1항 제1,2호에 언급된 정보로 구성
3) 검증된 정보 : 당국에 의해 전자적으로 검증된 개인정보
4) 기술 플랫폼 :사용자의 모바일 단말
5) 디지털 ID 인증서 : 제3조에 따른 인증서
6) 신뢰당사자 : 디지털 신분 등 또는 해외 디지털 거래 도구의 소유자가 자신의 신원 또는 확인된 정보를 보여주고 정보의 정확성을 확인해야 하는 자연인 또는 법인
7) 대면서비스 : 신원 또는 확인된 정보가 신뢰할 수 있는 당사자에게 보여지는 방식으로 디지털 신분증 소지자가 개인적으로 존재하는 비즈니스 거래
8) 전자신원확인 및 신뢰서비스에 관한 EU의 규정 : 전자거래를 위한 내부 시장의 전자 신원 확인 및 신뢰 서비스에 관하 유럽 의회 및 이사회의 규정 (910/2014)
9) 보증 수준 : 유럽 집행위원회 시행 EU 규정(2015/1502) : 유럽 의회 및 이사회에서 제공한 내부 시장의 전자신원 확인 및 신뢰 서비스에 관한 규정의 제8조제3항에 따라 보증 수준에서 사용하기 위해 전자적 방법으로 최소 사양 및 절차를 확인

제3조 (디지털 ID 서비스 등록 기관) 디지털 인구정보국은 디지털 ID 등록기관이다. 디지털 인구정보국은 디지털 ID 서비스의 생산과 관련하여 처리된 개인정보를 제3자에게 양도할 수 없다.

제2장 정보시스템의 필수 요구사항 및 평가

제4조 (디지털 신원정보 시스템) 디지털 인구정보국의 임무는 전자거래 또는 대면 거래에서 확인된 정보를 표시하는데 사용할 수 있는 모바일 응용 프로그램 및 관련 배경 시스템으로 구성된 디지털 신원 정보 시스템(이하 정보시스템)을 생성하는 것이다. 정보시스템의 목적은 디지털 신분증법에 의거하여 외국인의 전자 거래 도구 및 디지털 신분증의 제작 및 사용을 가능하게 하는 것이다.

제5조 (품질 및 정보 보안 요구사항) 정보시스템은 항상 사용 가능해야 하며 중단 시 필요한 백업 시스템이 있어야 한다. 디지털 인구정보국은 행정적, 기술적 조치를 통해 해당 정보를 관리해야 한다. 시스템 정보 보안에 대해 다음을 수행한다.

1. 정보시스템과 그 안에서 처리되는 정보는 사용 권한이 있는 사람만 사용 가능
2. 정보 및 정보시스템은 권한이 있는 사람이 아닌 다른 사람이 변경 불가
3. 정보 및 정보시스템은 사용 권한이 있는 사람만 사용 가능
4. 정보시스템은 예상되는 지능형 정보보안 위협을 예방할 수 있어야 함
5. 정보시스템에 대한 중대한 보안 위반 및 위협을 감지할 수 있어야 함

디지털 인구정보국은 정보시스템의 보다 상세한 기술 요구사항 및 정보보안 요구사항을 결정한다. 요구사항은 일반적으로 알려진 국가 또는 국제표준을 기반으로 해야한다. 디지털 인구정보국은 데이터 보안 요구사항에 대한 결정을 내리기 전에 핀란드 교통국과 상의해야 한다.

제6조 (식별 시스템 요구 사항) 정보시스템은 최소한 전자식별 및 신탁 서비스에 관한 EU규정 제8조제2항 B호에 언급된 강화된 보안 수준의 요구 사항을 충족해야 한다. 정보시스템은 외국 디지털 거래 도구의 생산에서 하위 섹션 1에 언급된 증가된 보증 수준에 따라 등록 요구사항을 충족할 필요가 없다.

제7조 (특정 정보를 보고할 의무) 정보시스템을 도입하기 전에 디지털 인구정보국은 다음 정보를 게시해야 한다.

1. 운영 개시일
2. 정보시스템의 특성과 정보시스템을 사용하는 당사자에게 제공되는 기술 인터페이스 및 테스트 준비에 대한 설명
3. 적합성 평가 수행
4. 기타 운영에 필요한 모든 조건

디지털 인구정보국은 제1항에 언급된 정보를 지체없이 보고 해야 한다. 이때 운영 중단이 발생한 경우에도 보고를 해야 한다.

제8조 (위협 및 방해에 대한 알림) 디지털 인구정보국은 기밀 유지 규정에 관계없이 과도한 지연 없이 디지털 ID 서비스 사용자에게 기능, 데이터 보안 또는 서비스 사용에 대한 중대한 위협이나 중단 또는 서비스 중단에 대해 알려야 한다. 통지서에는 위협이나 교란과 싸우기 위해 다양한 당사자가 처분할 수 있는 조치와 이러한 조치로 인해 소요되는 예상 비용을 설명해야 한다.

통지서에는 위협 또는 방해의 예상 기간이 명시되어야 한다. 또한 디지털 인구정보국은 위협 또는

방해의 종료를 디지털 ID 서비스 사용자에게 알려야 한다.

제9조 (적합성 평가) 정보시스템의 준수 여부는 정보보호 평가 기관에 관한 법률(1405/2011) 제2조에 따른 정보보호 평가 기관에서 발급한 인증서로 증명되어야 한다. 정보보호 평가 기관은 이 법 및 정보보호 평가 기관에 관한 법률에 따라 정보시스템 제공자의 신청에 따라 정보시스템이 해당 요건을 충족하는 지 여부를 평가한다. 평가 기준은 이 법과 디지털 인구정보국에서 정하는 기준에 의하여야 한다. 정보보호 평가 기관은 수행한 평가 인증서와 관련 검사보고서를 제공해야 한다. 디지털 인구정보국은 핀란드 교통 통신국의 평가를 위해 진술을 요청해야 한다.

평가 기관에서 발급한 인증서의 유효기관은 최대 2년이다. 정보보호 평가 기관은 비밀유지 규정에 관계 없이 공인인증서의 평가, 작성 및 유지에 필요한 모든 정보를 디지털 인구정보국에 요구할 수 있다. 인증서 발급에 대해서는 정보보호 평가 기관에 관한 법률 제9조 제3항을 별도로 적용한다.

제3장 핵심 신원증명

제10조 (핵심 신원증명) 디지털 인구정보국의 역할은 섹션 13에 따라 거래 수단에 포함된 핵심 신원증명 및 디지털 ID법 섹션 3에 따라 디지털 ID를 생성, 제공 및 관리하는 것이다. 핵심 신원 증명은 증명을 통제하는 사람이 정보시스템에 등록된 핵심 신원에 포함된 신원임을 보여주는 기술적으로 신뢰할 수 있는 방법이다.

핵심 신원증명에는 다음 정보가 포함된다.

1. 디지털 인구정보국의 인구정보시스템 및 인증서비스에 관한 법률 제11조 a에 따른 식별코드
2. 일련번호
3. 증거발행 국가
4. 증명의 유효기간
5. 증거보유자의 공개 키
6. 증거 서명자의 세부사항

핵심 신원증명은 최소한 전자신원 확인 및 신탁 서비스에 관한 EU 규정 제8조제2항b호에 언급된 보안 수준 향상의 요구 사항을 충족한다.

제11조 (핵심 신원증명 등록) 디지털 인구정보국은 외국의 디지털 거래 도구나 디지털 신분증에 관한 법률에 따른 디지털 신분증을 사용하는 경우 핵심 신분증을 등록한다.

핵심신원증명은 핵심신원증명 등록 서비스에서 생성된다. 디지털 정보 보호국은 개인 카드법(663/2016)의 제31조에 언급된 신분증 등록부 또는 여권등록부에서 개인의 여권 또는 신분증의 유효성 정보를 받을 권리가 있다.

핵심 신원증명의 유효성을 결정하기 위한 핵심신원증명 등록의 전제조건은 그 사람이 인구정보시스템에 등록되어 있다는 사실 외에도 여권법(671/2006) 제29조 규정에 명시된 수준이다.

제12조 (핵심 신원증명의 유효성) 핵심신원증명의 유효기간은 핵심 신원증명 등록의 근거가 된 신원문서의

유효기간이 만료된 후 1년이 지나면 만료된다.
디지털신분증의 경우 여권법 또는 신분증법에 따라 발급된 신분증명서를 말한다.
외국인의 디지털 거래 수단과 관련하여서는 정보시스템 및 디지털 인구정보국의 인증 서비스에 관한 법률 제9조a에 언급된 원격 등록을 기반으로 한 문서를 의미한다.

제13조 (핵심 신원증명에 관한 기록)) 주민등록번호부에는 정보시스템 및 디지털 인구정보국의 인증업무에 관한 법률 제11조에 따른 식별코드와 그 밖에 증거 이용에 필요한 기술적 정보가 저장되어 있다. 사람과 연결된 기술 플랫폼 등록부(장치 등록부)에는 사람의 고유한 식별정보, 사람과 연결된 기술 플랫폼의 기술 데이터, 장치 데이터 및 기타 핵심신원을 증명하는데 필요한 정보가 저장된다.

제4장 외국인의 디지털 거래 도구

제14조 (외국인의 디지털 거래도구) 디지털 인구정보국의 임무는 외국인을 위한 디지털 거래 도구를 만드는 것이다. 외국인의 디지털 거래 도구는 디지털 거래에서 신원 및 기타 확인된 정보를 표시하기 위한 거래 도구이며 정보시스템의 도움으로 사용하도록 제공된다. 디지털 인구정보국은 해외 디지털 거래 도구를 외국에 발급할 수 있다. 제10조에 해당되는 핵심 신원 증명인 핀란드 시민의 개인식별번호도 해외 디지털 거래 도구에 포함된다.

제15조 (해외 디지털 거래도구 발급) 디지털 인구정보국은 디지털 인구정보국에서 직접 거래하거나 인구정보 시스템법 및 Digi에 관한 법률 제9a조에 규정된 원격 등록 절차와 관련하여 외국인 디지털 거래 도구를 발급한다.

제16조 (해외 디지털 거래도구에 포함된 정보) 디지털 인구정보국은 외국 디지털 거래도구 보유자가 자신을 관리할 수 있도록 자신과 관련된 인구정보 시스템 데이터 사본을 제공한다. 거래수단 보유자에게 제공되는 정보는 다음과 같다.

1. 이름
2. 성
3. 생년월일
4. 개인식별번호
5. 생년월일로부터 파생된 연령증명

디지털 인구정보국은 정보를 본인에게 전달하기 전에 정보를 확인할 의무가 있으며, 이를 통해 정보를 제공한 당사자가 핵심신원 정보의 정확성 및 최신성을 확인할 수 있다. 디지털 인구정보국은 정보가 외국 디지털 거래도구의 소유자에게 전달된 후 개인에게 제공된 확인된 정보를 처리할 권한이 없다. 또한 외국인의 디지털 거래 도구에는 최초 신원 확인 방법에 대한 정보가 포함되어 있다.

제17조 (디지털 거래에서 확인된 정보 표시) 디지털 거래에서 외국 디지털 거래 도구의 소유자는 신뢰할 수 있는 담당자에게 보여주고 싶은 검증된 정보를 선택한다. 다만, 디지털 거래와 관련하여 최초 본인

확인 방법에 관한 정보는 항상 공개하고 있다.

제18조 (외국인 디지털 거래 도구 등록) 디지털 인구정보국의 임무는 외국인의 디지털 거래 도구 소유자 및 디지털 거래 도구 제공 및 생산을 위한 디지털 거래 도구의 유효성에 대한 등록부를 유지하는 것이다.

제19조 (해외 디지털 거래 도구의 유효성) 해외 디지털 거래 도구는 핵심 신원 증명의 유효기간 내에서만 유효하다.

제20조 (해외 디지털 거래도구 취소) 외국인의 디지털 거래 도구는 그 안에 포함된 핵심 신원 증명을 취소함으로써 취소된다. 디지털 인구정보국은 소유자의 요청에 따라 거래 도구를 취소한다. 디지털 인구정보국은 외국인의 전자거래 도구를 발급 받은 자 이외의 자가 사용하거나 사용하고 있다고 의심되는 사유가 있는 경우나 그렇지 않으면 거래 도구 사용의 보안이 손상될 경우 신청 없이 외국인의 전자거래 도구를 취소하거나 사용을 금지할 수 있다. 디지털 인구정보국은 거래 도구의 취소 또는 금지, 그 시기 및 사유를 부당한 지체없이 보유자에게 통지하여야 한다. 디지털 인구정보국은 요청 없이 이루어진 취소에 대해 결정을 내려야 하며, 외국 전자거래 도구 보유자에게 결정 및 정정 신청 가능성을 알려야 한다.

제5장 기타 조항

제21조 (디지털 ID 관리 서비스) 디지털 인구정보국의 업무는 「신분증에 관한 법률」에 따른 디지털 신분증 및 해외 디지털 거래 도구를 관리하기 위한 공식 디지털 ID 관리 서비스를 제공하는 것이다.

1. 디지털 신분증 또는 외국인의 디지털 거래 도구를 활성화
2. 디지털 신분증 또는 외국인의 디지털 거래 도구를 기술 플랫폼에 연결
3. 디지털 신분증 또는 외국인의 디지털 거래 도구를 취소

행정 공동 역무에 관한 법률(223/2007) 제6조에서 규정하고 있는 합동역무업무 외에 디지털 인구정보원은 외국인의 전자정보 관리와 관련된 보조업무를 부여할 수 있다. 공동서비스에서 수행할 거래 도구 작업에는 하위 제1항 제1~3호에 다른 작업이 포함될 수 있다.

추가 조사 후에도 공동서비스 계약자가 소유자의 요청에 따라 소유자의 신원을 활성화 또는 거래 도구에 연결하거나 거래 도구를 취소할 수 없는 경우 해당 문제를 디지털 인구정보국에 회부 해야 한다.

제22조 (판독인터페이스 및 검사 애플리케이션) 디지털 인구정보국의 임무는 비즈니스 거래에서 디지털 ID의 신원 및 확인된 정보를 확인하기 위한 판독인터페이스 및 검증 애플리케이션을 제작하는 것이다. 디지털 인구정보국은 다른 당사자가 작성한 검사 신청서도 수락할 수 있다.

판독 인터페이스는 방문 거래 시 신원 확인 및 확인된 정보를 확인하기 위해 사용한다.

디지털 인구정보국은 다른 당사자가 작성한 검사 신청서에 대한 요구사항에 대한 보다 자세한 규정을 발행한다. 요구사항은 디지털 인구정보국의 자체 판독인터페이스에서 요구하는 것과 유사한 수준의 정보보안을 요구해야 한다.

〈 참고 : 타 EU국의 전자 식별 전략 제도 〉

1. 덴마크

(1) 추진 근거 : 디지털 전략 2016-2020 문서, 디지털 신원을 위한 미래 인프라 문서에 따라 추진한다.

(2) NemID(전자식별 시스템) : 공공 부문과 덴마크 은행이 함께 개발한 전자식별 시스템으로 공공·민간 분야 모두에서 온라인에서 식별을 수행하고 있다.

(3) MetID(차세대 전자식별 시스템) : MetID는 NemID에 전자서명 기능, 모바일 기반 사용성 강화, 암호 및 물리적 인증을 통한 보안 기능을 추가했다. 주로 모바일이나 태블릿의 애플리케이션에서 사용되지만 일회용 암호를 사용하는 MitID 코드 표시, 시각장애인을 위한 MitID 오디오 코드판독기 등을 통해서도 사용가능하다.

(3) NemLog-in(전자식별중개솔루션) : 국가는 NemID·MitID를 중개하고 서비스제공자는 NemLog의 ID를 인증에 사용된다. 국민들은 1회 로그인으로 지자체, 덴마크 공공서비스 포털(Borger.dk) 등 공공과 민간의 다양한 서비스에서 사용 가능하다.

(4) 민간 솔루션 승인 여부 : 민간 솔루션도 사용할 수 있다.

2. 에스토니아

(1) 추진 근거: '국가 안보개발계획 2020-2030' 에 따라 보안을 고려한 안정적이고 지속가능한 신원 관리 시스템을 목표로 추진한다.

(2) 전자식별 도구: 전자식별 도구는 자연인에게만 부여되고 고급 전자적 기능을 갖춘 물리적 ID카드와 디지털ID가 있으며 디지털ID는 다시 온라인ID와 모바일ID로 나뉜다. 국민들은 전자식별 도구를 외교관 카드 및 거주 허가증 이용, 전자서명 생성 목적으로 활용할 수 있다.

(3) 디지털 신분증 : 15세 이상의 모든 시민에게 신분증을 의무 발급하는 에스토니아는 디지털 신원 프레임워크에서 규제기관이자 디지털 신원 제공자로 주도적 역할을 한다. 정보시스템 당국(RIA)이 전자 신원을 형성하고 개발하며 칩이 부착된 물리적 ID카드를 발급해준다. 향후에는 생체 인식 식별자 도입과 타국가 통용 전자신분증 발급을 계획 중이다.

(4) 민간 솔루션 승인 여부 : 민간의 전자식별 도구도 1종 정도 사용할 수 있다.

3. 노르웨이

(1) BankID : 은행에서 사용하는 공통 전자 식별 시스템이다. 인증 및 서명을 위한 모든 사용자의 개인 키가 중앙 집중식 서비스에 저장되는 공통 인프라를 기반으로 하며 원격 서명 서비스를 제공한다. 모든

BankID 발급자는 승인된 신탁 서비스제공자여야 한다. BankID의 모바일 버젼은 텍스트 형식의 짧은 명세서에만 서명할 수 있다.

(2) MinID : 정부가 만든 BankID의 대체 솔루션으로 공공서비스에서 활용되는 전자 식별 시스템이다.

(3) ID-porten : 공공기관에서 사용하는 로그인 포털로 2020년부터 약 2000개의 온라인 서비스에 대한 액세스를 제공하고 공공 민간의 여러 로그인 방법을 통해 국가에서 만든 중앙 전자 서명 및 워크플로 포털에 로그인을 할 수 있게 한다.

4. 네덜란드

(1) DigiID : 자연인을 위한 전자식별 시스템으로 사용자 이름과 비밀번호, 문제, DigiID 모바일 애플리케이션을 통한 선택적 추가 확인을 통해 개인을 식별한다. 공공분야에서도 의무적으로 사용해야 하는 것은 아니다.

(2) eHerkenning : 법인을 위한 전자식별 시스템으로 민간과 공공의 솔루션 혹은 민간과 공공이 협력하여 개발한 솔루션 중 하나를 선택하여 사용할 수 있다.

(3) 디지털신분증 : 물리적 신분증으로 NFC기술이 탑재되어 있으며, 카드를 스캔하여 DigID 계정으로도 민감한 서비스와 정보를 이용할 수 있다.

5. 독일

(1) 추진근거 : 연방경제 에너지부는 '디지털 전략 2025'의 다섯 번째 단계에 따라 전자식별의 국제적 도입을 위한 기초 마련, EU에서의 안전하고 신뢰할 수 있는 전자거래에 대한 표준 설정을 추진하고 있다. 또한 'Digital Germany'의 9개 계획 중 3번째 방법으로 전자신원을 확립하고자 하였다. 그 밖에도 전자식별 촉진에 관한 법률 및 전자 신분증에 대한 법률을 제정하는 등 법적 근거에 따라 디지털 신분증을 추진 중이다.

(2) eID카드 : 2010년 최초의 국가 eID카드를 발행하고, 국가가 전자 식별 솔루션을 제공하였다. 한편 물리적 신분증에 침을 부착하여 공공·민간에서 전자적인 방법에서 자신을 식별하는데 사용할 수 있도록 하였다. 독일 거주 여부와 무관하게 16세 이상의 EU 국가 시민이면 10년 동안 발급받을 수 있으며, 온라인이나 스마트폰을 통해 사용할 수 있다. 우편이나 은행 등에도 사용 가능 하나 여권으로는 사용할 수 없다. 향후의 모바일 eID 도입을 통해서 향후에 서비스의 수를 확장하는 것이 목표이다.

(3) 민간 솔루션 승인 여부 : 민간 솔루션도 사용가능하나 eID카드 보다는 기능이 낮다.

Ⅲ 시사점

❍ 핀란드는 본 입법을 통해 '핵심 신원증명 - 신분증 - 디지털 신분증 - 디지털 신분증명 서비스'로 이어지는 일련의 디지털 신원증명 과정 상 필요한 입법을 일괄하여 추진

- 디지털 신분증에 관한 법률에서는 모바일 등을 통해 오프라인에서도 활용할 수 있는 디지털 신분증이 포함하는 정보, 유효성, 활성화 과정 등을 면밀히 기술

- 한편 디지털 신원인증에 관한 법률에서는 디지털 신분증에 식별코드를 통해 디지털 환경에서 신원인증 서비스제공에 필요한 발급자의 정보시스템의 요구사항, 외국인의 사용 등에 대한 사항을 입법 내용에 포함

❍ 국내에서도 디지털 운전면허증을 필두로 디지털 신분증의 도입을 시도 중이며 국내에서도 후속 디지털 신분증 정책을 추진할 때 핀란드의 입법 내용을 주목할 필요가 있음

- 국내법에서는 주로 플라스틱 신분증을 대신하여 동일한 효력을 가진 디지털 신분증 시행 근거만 담고 있을 뿐 디지털 신분증의 특성을 반영하고 있지는 않음

- 국내에서는 모바일을 활용한 디지털 신분증 도입 단계에 들어선 만큼, 향후 디지털 신분증과 디지털 신원인증과의 연계에 대한 정책 사항과 입법 시에도 고려 가능

❍ 다만 국내의 경우 개별 신분증의 개념이 파편화되어 있으므로 디지털 신분증과 디지털 신원인증에 관한 입법내용은 참고하되, 입법 체계에 대한 심도있는 고민 필요

〈 참고 : 국내 주요신분증 근거법 〉

신분증	근거법	부처
공무원증	국가공무원 복무규칙 제4장(공무원증)	인사혁신처
주민등록증	주민등록법 제24조(주민등록증의 발급 등)	행정안전부
여권	여권법	외교부
운전면허증	도로교통법 제85조(운전면허증의 발급 등)	경찰청
장애인등록증	장애인 복지법 제32조(장애인등록)	보건복지부
⋮	⋮	⋮

디지털 신원인증 2 모나코, '디지털 신원 인증법' 제정

Ⅰ 개요

❍ 모나코 국왕은 디지털 도구를 보다 쉽고 안전하게 사용할 수 있는 디지털 ID 정책을 실시(2021.6.28.)하기 위해 그에 앞서 디지털 신원 인증법*을 제정(2019.12.17.)

* Loi n° 1.483 du 17 déembre 2019 relative àl'identitéuméique.[3)]

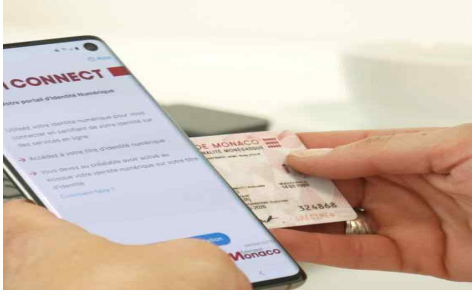
- 디지털 ID는 보안카드에 전자인증서 형식의 ID가 포함되어 있어 온라인에서 본인의 신원인증과 개인의 온라인 서명에 활용되는 새로운 신원인증 방법

❍ 모나코 국민이나 거주자는 시청 직원이나, 거주지 인근의 셀프 서비스 대화형 단말기를 통해 보안카드를 발급 받고 PIN번호를 설정하면 디지털 신원을 활성화 할 수 있음

- 디지털 ID는 보안카드 형태의 신분증을 발급받고, 카드리더기를 활용하거나 휴대폰에 디지털 ID를 설치해서 온라인에서 신원을 확인

- 디지털 ID를 통해 확실한 신원확인이 가능하고, 사용자의 시간을 절약할 수 있으며, 사용자 ID와 암호의 수를 줄여 개인정보 보호에도 탁월

〈 참고 : 모나코의 디지털 ID(M Connect) 사용법 〉



※ 출처 : 모나코 m connect 소개 페이지(https://mconnect.gouv.mc/en/learn-more)

---

3) ttps://journaldemonaco.gouv.mc/Journaux/2019/Journal-8466/Loi-n-1.483-du-17-decembre-2019-relative-a-l-identite-numerique

Ⅱ 주요 내용

❍ 디지털 신원 인증법은 크게는 디지털 ID에 대한 정의, 개인정보의 보호, 등록시스템 담당자의 역할, 정보주체의 권리 등에 대한 내용으로 구성됨

- 국가가 생성하는 디지털ID는 모나코 국적의 모든 자연인, 모나코 공국 내에서 정해진 조건에 따라 입국 및 거주 허가를 받은 외국 국적의 자연인에게 할당됨

- 디지털ID의 생성 및 할당은 국가 독점적 권리가 아니라 민간에서도 생성하여 자연인 또는 법인에게 할당할 수 있음

〈 법률에 등장하는 주요 정의 〉

디지털 식별	자연인 또는 법인을 고유하게 나타내는 전자 형식의 개인식별 데이터를 사용하는 프로세스
개인 식별정보	자연인 또는 법인의 신원을 확인할 수 있는 정보의 집합
디지털 신원인증	자연인 또는 법인의 디지털 식별을 확인하는 전자 프로세스
디지털 ID	개인 식별정보를 포함하고 온라인 서비스 인증에 사용되는 유형 및 무형의 요소
디지털 식별자	개별 여부에 관계 없이 신원 제공자가 제공한 문자, 숫자 또는 기호의 조합으로 자연인 또는 법인을 명확하게 나타내는 방법
생체 인식정보	얼굴 이미지 또는 검시 정보와 같이 고유한 식별을 허용하거나 확인하는 자연인의 신체적, 생리적 또는 행동적 특성과 관련된 특정 기술 처리로 인한 개인정보
식별가능한 자연인	이름, 식별 번호, 위치 데이터, 온라인 식별자 또는 그의 신체적, 생리적, 유전적, 심리적, 경제적, 문화적 또는 사회적 정체성과 관련된 보다 구체적인 요소
민감정보	고유한 자연인을 식별하기 위한 생체정보, 유전정보 또는 건강 또는 성생활 정보 및 직·간접적으로 의견이나 정치적, 인종적, 또는 민족적, 종교적, 철학적 또는 노동조합 가입을 드러내는 정보
신분증 제공자	자연인 또는 법인의 식별을 담당하는 유자격 또는 무자격 신탁 서비스 제공자, 전자 식별 수단의 발급 및 해당 식별 수단에 해당하는 식별정보의 주기 수명 유지 및 관리를 담당하는 서비스 제공자
디지털 식별시스템	디지털 식별수단을 자연인 또는 법인 또는 법인을 대표하는 자연인에게 발급하는 전자식별 시스템
신탁 서비스	본인확인, 본인인증, 서명, 스탬프, 타임스탬프, 웹사이트인증 및 이에 관한 증명서 등으로 구성되며, 유료 또는 유료로 제공되는 전자적 서비스

❍ 디지털 신원 인증법은 신원 인증의 중요도에 따라 기술 사용, 표준 및 기술을 기준으로 총 3가지(낮은수준, 상당한 수준, 높은 수준)로 분류하여 최소 필요의 인증만 이루어지도록 함

- '낮은 수준의 보증'은 청구된 신원에 대해 제한된 수준의 신뢰성을 부여하거나 개인의 것으로 간주되는 전자 신원확인 수단을 의미
- '상당 수준의 보증'은 기술 사양을 기반으로 개인의 청구 또는 주장된 신원에 상당한 정도의 신뢰성을 부여하는 전자 식별 수단에 해당
- '높은 수준의 보증'은 실질적인 기술 제어를 바탕으로 개인의 청구 또는 주장된 신원에 더 높은 수준의 신뢰성을 부여하는 전자 식별수단을 일컬음

❍ 모나코 공국이 개인정보를 통해 디지털 신원 인증을 담당하는 데 신뢰를 형성할 수 있도록 디지털ID 등록시스템의 개인정보 관리 원칙을 천명

- 디지털 ID에 활용되는 개인정보 보호가 신원 인증의 공신력을 담보하는 만큼 개인정보 오남용 금지, 보호조치, 정확성 보증, 보유기간 등을 명확히 함

〈 디지털 신원 인증법에 나타낸 개인정보 보호 조항 〉

권리	해당 조문
개인정보 오남용 금지	모나코 디지털 ID 등록시스템에 포함된 정보는 의견, 인종 또는 민족, 정치, 종교, 철학 또는 노동조합 구성을 결정하거나 건강, 유전적 특성, 성적 지향, 성생활과 관련된 정보를 얻는 목적으로 사용할 수 없다.(제7조)
디지털 ID 개인정보의 보호	제4조, 제5조에 따라 모나코 디지털 ID 등록시스템에는 디지털ID가 생성 및 할당된 자연인의 식별에 필요한 개인정보 및 개인식별 자료만 기록 저장된다. 원칙적으로 민감정보의 보유는 금지된다. 모나코 디지털 ID 등록시스템에 기록 저장되는 개인정보 및 개인식별정보 목록은 주권에 따라 게시된다.(제8조)
디지털 ID 개인정보의 정확성 보증	모나코 디지털 ID 등록시스템 지원 문서를 기반으로 기록된 정보의 정확성은 보장된다. 다른 모든 정보는 순전히 제공하는 데이터로 처리된다.
디지털 ID 개인정보 보유기간	모나코 디지털 ID 등록시스템에 저장된 정보의 보유기간은 수집 목적에 필요한 기간을 초과할 수 없다. 이 기간이 지나면 정보는 공익을 위한 보관 목적(과학적 또는 역사적 연구 목적 또는 일반적인 관심의 특성을 나타내는 통계)으로만 보관된다.

❍ 모나코 공국은 디지털 신원 인증법에 디지털ID를 사용하는 정보주체의 구체적인 권리(열람권, 피통지권, 정보접근권)도 조문화하여 두텁게 보호하고 있음

〈 디지털 신원 인증법에 나타낸 정보주체의 주요 권리 〉

권리	해당 조문
열람권 (제13조)	제1항 디지털ID 등록시스템에 기록된 하나 이상의 정보를 알고자 하는 공공 및 민간은 해당 레지스터를 관리하는 담당자에게 열람을 요청해야 한다. (...) 제3항 디지털ID 등록시스템 담당자는 정보주체가 사전에 명시적으로 동의한 경우에 한하여 전 항의 데이터 외의 데이터를 요청자에게 전달할 수 있다.
피통지권 (제14조)	디지털ID 등록시스템 담당자는 기록된 하나 이상의 정보를 수집하는 자연인 또는 법인은 정보에 접근하고 수정할 권리가 있음을 통지하여야 한다.
정보 접근권 (제15조)	자연인 또는 법인은 개인정보 보호에 관한 법률에서 제공하는 조건에 따라 디렉토리에 포함된 정보에 엑세스하고 수정할 권리가 있다.

〈 참고 : 디지털 신원에 관한 법률의 조문 구성 〉

제1조 용어정의	제11조 등록시스템 담당자의 관리 의무
제2조 디지털 ID의 구성	제12조 등록시스템 담당자의 비밀보장 의무
제3조 디지털 ID의 보증 수준	제13조 정보주체의 열람권
제4조 디지털 ID 생성 대상	제14조 정보주체에 대한 통지의무
제5조 디지털 ID 할당	제15조 정보주체의 정보 접근권
제6조 디지털 ID 등록 시스템	제16조 디지털 ID의 상호 연결
제7조 디지털 ID 개인정보 오남용 금지	제17조 디지털 ID 제공자의 책임
제8조 디지털 ID 개인정보의 보호	제18조 정보주체의 열람권
제9조 디지털 ID 개인정보의 정확성 보증	제19조 개인정보 오남용에 대한 벌금
제10조 디지털 ID 개인정보 보유기간	제20조 예외조항

Ⅲ 시사점

❍ 모나코에서는 보안카드와 단말기를 통한 디지털 신원 인증방법을 채택하면서, 개인정보의 보호 방안을 최우선 시 하여 입법을 추진

- 모나코 디지털 신원인증법은 인증방법을 3가지로 체계적으로 분류하여 디지털 신원인증 사항이 발생했을 때 필요 최소한의 인증이 진행되는 것을 대전제로 함

- 디지털 ID 등록시스템 담당자 및 제공자의 책임있는 서비스제공을 요구하고 디지털 ID 사용에 대한 보유기간 설정, 통지권 및 열람권 등 정보주체의 권리를 입법으로 보장

❍ 디지털환경에서의 신원인증은 엄격한 보안을 요하므로 국내 공공 분야에서도 정보주체의 권리를 두텁게 보호하는 디지털 신원인증법 제정이 필요

- 기존의 신원인증은 주민등록번호, 주민등록증, 공공I-PIN 중심으로 진행되다가 전자서명 방법을 차용하여 공인인증서 중심으로 디지털 신원확인이 이루어짐

- 현재는 전자서명법 개정으로 공인인증서 대신 다양한 전자서명 방식이 디지털 신원확인에 쓰이고 있으며 최근에는 모바일 운전면허증를 디지털 신원인증 방법으로 도입

- 입법 현황으로는 전자정부법 제10조를 제외하고는 통일된 체계하에서 디지털 신원인증에 대한 내용을 다루는 뚜렷한 입법 움직임은 없는 상황

〈 참고 : 디지털 신원 관련 입법 현황 〉

법률명	조문 내용
전자정부법 제10조	① 전자서명법 제2조제2호에 따른 전자서명 및 ② 대통령령으로 정하는 방법
전자정부법 시행령 제12조	①「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제23조의3에 따른 본인확인 기관이 제공하는 본인확인의 방법 ② 행정기관의 장이 발급하는 전자적 방식의 신분증을 이용하는 방법
전자서명법 제2조제2호	2. "전자서명"이란 다음 각 목의 사항을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다. 가. 서명자의 신원 나. 서명자가 해당 전자문서에 서명하였다는 사실

디지털 신원인증 3 뉴질랜드, '디지털 ID 신뢰 프레임워크 법안' 제안

Ⅰ 개요

❍ 뉴질랜드 정부는 디지털 ID 신뢰 프레임워크 법안*을 제안하여, 안전하고 신뢰할 수 있는 방법으로 디지털 ID 서비스가 제공될 수 있도록 근거 법률을 의회에 제안함

* Digital Identity Services Trust Frmewok Bill[4](2021.9.29.)

- 디지털ID는 옵트인 인증체계*를 기반으로 정보주체의 통제 아래 자신이 누구인지 온라인에서 증명하고, 온라인 서비스에 접근할 수 있는 서비스를 의미

* 옵트인(Opt-In) 인증방식 : 당사자의 동의 하에 개인정보 수집, 활용에 대한 처리가 이루어지는 개인정보 처리 방식

- 본 프레임워크는 왕실 장관이 집행하며 개인이나 조직의 거래를 위한 디지털 ID 제공을 규제하기 위해 마련되었으며 2024.1.1. 발표 예정

- 기존에 적용되던 전자신원법(2012)이나 개인정보 보호법(2020)의 체계를 유지하면서도 디지털 ID라는 새로운 서비스에 대한 규정을 추가한 것이 특징

❍ 정부는 4,500건 이상의 의견 수렴과 청문회에서의 28명의 증언을 토대로 법안을 수정·보완하여 논리적 완결성을 더함

- 마오리족과의 협의 사항을 반영하여 평등한 의사결정이 되도록 하고 신뢰마크를 인증마크로 변환하여 인증된 서비스와 그렇지 않은 서비스 간의 식별이 용이하게 함

〈 참고 : 신뢰마크와 인증마크 〉

신뢰마크	인증마크
신뢰 프레임워크 준수하는 디지털 ID 서비스 제공자에게 부여하는 마크 ※ 인증·비인증 서비스의 구분이 쉽지 않음	신뢰 프레임워크 제공자가 아닌 인증된 서비스에 대해서만 발급되는 인증마크

4) https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/BILL_116015/digital-identity-services-trust-framework-bill

Ⅱ 주요 내용

❍ 디지털 ID 신뢰 프레임워크는 관리기관(이사회와 기관), 인증제도, 디지털 ID 제공 지침으로 구성

❍ 신뢰 프레임워크 이사회는 신뢰 프레임워크에 대한 지침을 제공하고 프레임워크의 성능과 효과를 모니터링할 책임과 권한을 가짐

- 이사회는 디지털 정보의 윤리적 사용. 프라이버시 및 기밀의 보호 등 전문적 지식을 가진 자나 마오리족과 관련된 자로 구성되어 투표를 통해 의사결정을 진행

- 디지털 ID 제공 지침은 본 법을 실행하거나 완전한 효력을 발휘하는데 필요한 세부적인 내용에 관한 것으로 신뢰 프레임워크 이사회에서 초안을 작성

- 지침은 크게 정보의 정확성을 결정하여 해당 정보를 안전하게 재사용할 수 있도록 개인 정보를 보호하고, 무단으로 수정되지 않도록 하는 등 당사자 간 정보 공유를 용이하게 함

❍ 신뢰 프레임워크 기관은 인증에 대해 발생된 불만이나 문제를 조사하고, 이사회가 정한 규칙을 시행하고 위반에 대한 구제책을 부여하는 등 인증에 대한 중요 결정을 내림

- 기관은 공공기관 직원과 개인 등 10명으로 구성되며, 국민이 디지털 ID와 관련하여 이의를 제기하는 경우

- 이사회는 디지털 정보의 윤리적 사용. 프라이버시 및 기밀의 보호 등 전문적 지식을 가진 자나 마오리족과 관련된 자로 구성되어 투표를 통해 의사결정을 진행

❍ 기관은 제3자를 평가자로 두고 인증기준(정보의 무결성 또는 평판의 유지 가능 여부)에 따라 서비스 제공자*를 평가하는 방식으로 인증제를 운영

* 서비스 제공자 : 1개 이상의 공인된 디지털 ID 서비스를 제공하는 자를 의미

- 서비스제공자가 이행사항을 위반*한 경우, 기관은 경고, 명령, 인증 정지 취소, 추가 기록 보관 또는 보고를 명할 수 있는 권한을 보유

※ 위반 사항 : 주요, 특정 정보를 제공하지 않은 경우, 정보 변경사항을 고지하지 않은 경우, 기관의 권한 행사를 방해하는 경우

Ⅲ 시사점

❍ 뉴질랜드 정부는 디지털 ID 신뢰 프레임워크 법안을 통해 디지털 ID의 안전한 활용에 필요한 정부의 역할을 법문으로 확고히 함

- 신뢰 프레임워크 기관은 법문에 따라 디지털 ID의 오남용 피해자의 구제제도를 마련하고, 디지털 ID 서비스 제공자의 인증제를 실시하여 감독자의 역할을 수행

❍ 디지털 신원 인증의 정보 주체의 정보 주권을 강화하기 위한 체계적인 구제 방법을 사전에 마련하는 것이 필요

- 정보 주체를 위해 서면 형태의 문제 제기, 시기적절하고 효율적인 문제 해결, 정보 주체를 위한 추가적인 지원책을 제시하는 적극적인 제도 수립 선행

- 문제 해결 기관 또한 문제의 신속 접수, 분쟁 절차 시행, 문제 발생이 예상되는 경우 사전 예비평가 수행 등을 체계적인 분쟁 해결 및 예방 절차 마련 역할 명시

❍ 민간이 제공하는 디지털 신원 인증 환경을 상정하고, 서비스 제공의 주요 원칙, 관리 감독 기준 등을 수립하여 이에 대한 입법 대비가 필요

- 최근 공공의 웹페이지에서는 민간의 전자서명 방식(카카오, KB국민은행, NHN 페이코, 패스)을 도입하여 본인인증 서비스를 진행 중

- 뉴질랜드에서의 민간 디지털 ID 제공 허용 사례과 최신의 민간 전자서명 방식 활용 트렌드를 비추어보아 민간 디지털 ID 서비스의 도입도 가시적

- 민간 디지털 ID 제공자와 공공의 디지털 ID의 병용 환경하에서 디지털 ID의 신뢰를 확보하는 것이 정책추진의 성패를 좌우할 수 있음

- 디지털 ID 서비스를 모니터링 할 수 있는 별도 기구 설치, 서비스 제공자 인증제 시행 등을 통해 책임성과 신뢰성을 담보할 수 있음

자동화된 의사결정 1 캐나다, '자동화된 의사결정에 대한 지침' 도입

Ⅰ 개요

❍ 캐나다 연방정부는 자동화된 결정 시스템이 법률에 의거하여 더욱 효율적이고 정확하며 일관된 결정을 내리도록 하기 위하여 '자동화된 의사결정에 대한 지침'을 도입'*

* Directive on Automated Decision-Making(2020.4.1.)[5]

- 본 지침의 도입으로 정부에서 내린 자동화된 결정은 데이터 중심적이고, 책임이 있으며 절차상의 공정성과 적법 절차를 준수하여야 한다는 대원칙을 명시

- 자동화된 결정을 내리기 전에는 알고리즘의 영향을 평가하여 부정적인 결과를 예방하고, 문제가 발생했을 때는 시스템에 대한 정보를 대중에게 제공하는 근거로 기능

〈 참고 : 자동화된 의사결정 〉

의의	자동화 시스템을 사용한 개인정보 처리에 기반한 의사결정으로 개인정보 처리의 의사결정 단계에서 사람의 개입이 배제된 경우를 의미
활용 분야	고용 결정, 사회복지 지급, 재범 위험성 평가, 시험평가 등
문제 배경	- 기존에도 교통질서 신호기, 학교 배정, 공공시설 출입 전자동화 등 의사결정 구조가 비교적 단순하고 결과예측이 가능한 자동화된 의사결정을 행정에 활용해오고 있었음 - 그러나 최근에는 인공지능의 알고리즘을 통해서 이루어지는 자동화된 의사결정은 의사결정 구조가 비정형적, 비구조적이게 됨에 따라 결과 예측이 어렵고 행정행위의 인과관계에 대한 설명이 어렵게 됨
문제	알고리즘으로 인한 편향 및 차별, 행정행위의 불투명성 및 부당한 결과 등
사례	[형사사법 분야의 자동화된 의사결정] 2016년 미국의 위스콘신주 대법원은 콤파스(Compas) 알고리즘의 평가지수를 통해 피고의 재범 위험을 평가한 것에 대해서 법원이 결정이 알고리즘만으로 이루어졌다면 위법이지만 보조적 수단으로 활용되는 경우에는 적법절차 위반이 아니라고 판시한 바가 있음. 자동화된 의사결정만으로 국민의 권리의무의 변동을 가져오는 처분 등의 행정행위가 이루어지는 것에 대한 위험성을 경계하는 판례

5) https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

Ⅱ 주요 내용

❍ 캐나다 정부는 자동화된 의사결정을 행정 서비스에 활용할 경우, 알고리즘 영향평가 시행, 투명성 보장, 품질 보증, 구제수단 마련, 시행 주요 내용 보고 의무 등을 명문화

- 자동화된 의사결정을 수행하려는 기관은 시스템을 생성하기 전에 알고리즘 영향평가를 선행해야 하며, 평가 결과를 대중에게 공개하고, 시스템에 반영해야 함

- 사전에 재무부가 지정한 웹사이트에는 자동화된 의사결정 시스템의 효과성과 효율성에 관한 정보를 게시하고, 문제 발생 시에는 피결정자의 이의제기 수단에 대한 선택권을 제시

❍ 자동화된 의사결정의 투명성을 확보하기 위해서는 결정 관련 사항 문서화 의무, 피결정자를 위한 통지의무, 설명 제공의무, 구성요소에 대한 접근 방법 확보 등 해당 기관의 의무 규정

- 자동화된 의사결정을 하려는 기관은 결정 전에는 자동화된 의사결정 수행 여부를 통지하고, 결정 후에는 결정이 내려진 방법과 이유에 대해 의미있는 설명을 제공해야함

- 캐나다 정부는 피결정자의 알권리로 자동화된 의사결정 시스템의 모든 배포 버전을 포함하여 접근하고 테스트할 권리를 보유해야 하지만 시스템의 구성요소가 무단으로 공개되지 않도록 노력해야 할 의무도 동시에 보유

- 의사결정 시스템의 소스코드는 secret, top secret, protected C로 분류하여 공개에 면제되거나 제외될 수도 있으며 이러한 결정은 최고 정보 책임자가 내림

❍ 또한 자동화된 결정의 품질을 보증하기 위해 테스트 및 모니터 절차 마련, 데이터 검증, 동료 검토, 직원 훈련, 비상계획 수립, 보안정책 마련, 법률 요구사항의 준수 등을 장치를 마련

- 자동화된 의사결정 시스템을 생산하기 전에 적절한 수준의 승인을 획득함은 물론 필요한 경우 인적 개입을 허용하도록 하여 피해의 최소화를 최우선화 함

〈 참고 : 기타 국가들의 자동화된 의사결정에 관한 입법례 〉

1. EU 일반 개인정보 보호 규정(GDPR; General Data Protection Regulation)

제22조는 개인에 대해 "법적 효과"를 생성하거나 "심각한 영향을 미치는 경우" 정보주체는 "완전히 자동화된 결정"의 대상이 되진 않을 권리를 가진다는 점을 명시한다. 또한 유럽 정보 보호 위원회는 EU 사법재판소의 최종 해석에 따라 완전히 자동화된 결정에 다음에 해당하지 않은 경우는 원칙적으로 금지한다.

1. 자동화된 의사결정은 해당 법률에 의해 승인되어야 한다.
2. 계약 체결 또는 이행에 필요한 목적으로만 사용이 가능하다.
3. 정보주체의 명시적 동의가 있어야 가능하다.

이때 정보주체가 회사 또는 사람의 개입에 대한 자신의 관점을 표현하고 결정에 이의를 제기할 권리를 포함하여 데이터 주체의 권리를 보호하기 위한 조치를 구현해야 한다.

특히 인종 또는 민족과 같은 특정 범주의 개인정보 사용에는 관련 논리에 대한 의미있는 정보 뿐 아니라 정보주체에 대한 처리의 중요성과 예상되는 결과까지 특정 제한을 둔다.

2. 브라질(LGPD; Lei Geral de Proteção de Dados)

브라질은 정보주체는 그들의 이익에 영향을 미치는 개인정보의 자동화된 처리만을 기반으로 내린 결정(개인, 직업, 소비자 및 신용등급 또는 성격 관련)에 대한 검토를 요청할 권리가 있다고 명시했다.

3. 미국 (캘리포니아 개인정보 권리법) ※ 2023.1.1. 시행

캘리포니아 주에서는 개인정보 보호국을 설립하고, 정보주체가 기업에 대한 열람권 및 거부권을 행사할 수 있는 규정을 채택한다. 이때 정보주체가 행사할 수 있는 열람권 및 거부권의 대상은 자동화된 의사결정 기술을 허용한 의사결정 과정이나 결과에 대한 내용을 포함한다.

4. 미국(콜로라도, 버지니아, 코네티컷 개인정보 보호법) ※ 2023. 시행 예정

콜로라도, 버지니아, 코네티컷 주에서는 개인이 소비자와 관련하여 "법적 또는 유사하게 중대한 영향을 미치는 결정을 촉진하기 위한 프로파일링"을 거부할 수 있도록 한다. 이미 기존에 옵트아웃 권리를 제공하지만 금융, 대출, 주택, 보험, 교육, 형사사법, 고용, 의료 등과 관련된 완전 자동화된 결정에 대해서는 거부권을 사용할 수 있다.

5. 캐나다(Québec Bill 64) ※ 2023.9. 시행

캐나다 퀘백주는 해당 법률을 통해 개인정보에 적용되는 자동처리에 기반한 결정 시스템을 규제한다. 회사는 개인에게 자동화된 결정을 시행할 경우 통지하여야 하며, 반대로 개인은 회사의 대표에게 결정에 사용된 개인정보, 결정요인 및 매개변수 등에 대한 열람을 요청할 수 있고, 나아가 완전 자동화된 결정에 사용된 개인정보를 수정할 수 있다.

Ⅲ 시사점

❍ 캐나다의 해당 지침은 단순 정책 결정 뿐 아니라 국민의 권리·의무에 변동을 발생시키는 행정 행위에도 자동화된 의사결정을 적극적으로 활용하는 경우를 상정하고 제정

- 인공지능을 활용한 자동화된 의사결정의 시행 타당성을 검토하는 영향평가, 시행 후 품질을 보증하는 절차 뿐 아니라 피결정자의 구체적인 권리구제수단 까지 포함

❍ 국내에서는 행정기본법에 따라 인공지능을 통한 자동화된 의사결정을 주로 정책 결정의 판단 근거를 확보하는 수단으로 활용하고 있는 것이 특징

- 행정기본법 제20조(자동적 처분)에 따라 처분*에 재량이 있는 경우를 제외하고 완전히 자동화된 시스템으로 처분 가능

* 처분 : 행정청이 구체적 사실에 관하여 행하는 법 집행으로서 공권력의 행사 또는 그 거부와 그 밖에 이에 준하는 행정작용

- 이에 따라 국내에서는 처분이 아니거나 재량행위가 아닌 분야 중심으로 자동화된 의사결정을 점차 공공분야에서 활용하는 사례가 증가

〈 참고 : 공공분야에서의 자동화된 의사결정의 활용 사례 〉

시행처	도입 사례	주요내용
부천시	CCTV 영상을 활용한 지능형 역학조사 시스템	CCTV 영상을 AI로 동시 분석하여 확진자·접촉자의 이동 경로를 세부적으로 추적
개인정보보호위원회	AI 개인정보 침해 예방 지원 시스템	인공지능이 개인정보보호위원회의 의결례, 판례 등에서 업무 특성에 따른 침해평가 근거와 평가 결과를 비교 및 분석하고 연관관계를 지속적으로 추론
경기도 교육청	AI 직무적합성 평가 시스템	1차 합격자를 대상으로 인공지능을 활용하여 교육 전문직원으로서의 직무 적합성을 여러 차원으로 검증

❍ 캐나다 사례처럼 기준 정립 후에는 국내에서도 처분에 재량이 있는 경우가 아닌 경우에도 자동화된 의사결정을 활용하여 행정 효율을 제고할 수 있을 것으로 예상

- 전자정부법 상에 국민을 위한 사후 권리 구제책 등을 마련하고 안전한 법률적 기반을 바탕으로 자동화된 의사결정을 행정에 접목하는 적극적 자세 요구