2022 Privacy Report

개인정보보호 월간동향분석

9월호

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2022 Privacy Report

개인정보보호 월간동향분석

9월호

1. 영국 정보주체 접근요청(DSAR) 현황과 시사점

2. 드론 이용 확산에 따른 개인정보보호 이슈 분석

3. 개인정보 국외이전 주요 정책 동향에 대한 OECD 분석과 시사점

KISA

영국 정보주체 접근요청(DSAR) 현황과 시사점

[목 차]

1. 영국 정보주체 접근 요청(DSAR) 개요

▶ **(개념)** 정보주체로서의 권리 보호 차원에서 개인정보에 대한 접근 및 열람을 요청하는 행위를 '정보주체 접근 요청(Data Subject Access Request, 이하 'DSAR')'이라 함

- EU GDPR 및 UK GDPR*은 정보주체인 개인에게 개인정보 컨트롤러가 보유한 자신의 개인정보에 대한 접근 권한을 부여함으로써, 개인이 자신의 정보가 어떻게 또는 적법하게 처리되는지를 확인할 수 있도록 함(GDPR 제15조)

* 양 규정은 기본적으로 동일한 체계로 구성되며, 이하 구분이 필요 없을 경우는 'GDPR'로 통칭

▶ **(정보주체의 신청)** 영국 개인정보보호 법률 체계 하의 정보주체는 구두 또는 소셜 미디어를 포함하여 서면으로 DSAR 신청 가능(영국 개인정보감독기구(ICO) 권장사항[1])

- 이때 신청 개인은 특정 형식의 어휘를 사용하거나, 법률을 참조하지 않아도 되며, 특정 연락처로만 보낼 필요도 없음
- 해당 개인은 제3자(예: 친척, 친구 또는 변호사)를 통해 대리로 DSAR 신청이 가능하며, 온라인 포털 상에서도 개인을 대신하여 DSAR 답변을 수령할 수 있음
- 다만, 이 경우 제3자는 개인의 권리를 대리한다는 사실을 입증할 수 있어야 함

▶ **(컨트롤러의 대응)** GDPR 하에서는 대응 일정이나 미대응에 따른 처벌 규정을 둠으로써 정보주체의 신청 절차에 비해 컨트롤러의 대응 절차를 한층 까다롭게 규정

- 컨트롤러 조직은 정보주체의 DSAR 신청 건에 대해 기본적으로 무료로 정보를 제공해야 하며 대응 시간도 1~3개월 이내로 제한(GDPR 제12조제3항)
- DSAR에 적절히 대응하지 못할 경우 해당 컨트롤러 조직은 최대 2,000만 유로 또는 글로벌 연매출 4% 중 많은 쪽을 행정 과징금으로 내야 하는 등 강도 높은 규제를 받게 됨(EU GDPR 제83조, UK GDPR 제157조)

▶ **(정보접근권의 보장)** 개인정보 컨트롤러는 제3자의 권리와 자유를 침해하지 않는 범위 내에서 정보주체에게 처리가 진행 중인 개인정보의 사본을 제공할 의무를 지님(GDPR 제15조제3항, 제4항)

- 일반적으로 컨트롤러는 이러한 정보를 무료로 제공해야 하나, 정보주체가 요청한 추가 사본에 대해 또는 요청이 명백히 근거가 없거나 과도할(manifestly unfounded or excessive) 경우 합리적인 행정 수수료를 부과할 수 있음
- 한편, 개인정보가 제3국 또는 해외 조직으로 이전되는 경우, 정보주체는 이전과 관련된 적절한 안전장치에 관한 설명을 통보받을 권리가 있음

1) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

2. DSAR 적용 시 고려 사항

(1) 신원 확인 및 정보수집

▶ DSAR이 접수되면 잘못된 수신자에게 개인정보를 공개하는 일이 발생하지 않도록 컨트롤러는 우선 DSAR 신청자의 신원을 확인해야 함(GDPR 전문 제64조*)

* "컨트롤러는 특히 온라인 서비스 및 온라인 식별자와 관련한 상황에서 열람을 요구한 정보주체의 신원을 확인하기 위한 모든 적정 조치를 취해야 한다."

▶ 컨트롤러가 개인정보 주체 식별이 불가능함을 입증할 수 있는 경우, DSAR에 대한 조치를 거부할 수 있음(GDPR 전문 57조)

- 컨트롤러는 DSAR을 신청한 사람의 신원에 대해 합리적인 의심이 생기면, 추가 정보를 요청할 수 있음(제12조제6항)
- 컨트롤러는 필요한 경우 규제기관인 ICO에 대해 컨트롤러가 취한 조치를 정당화할 수 있도록 미대응 결정에 대한 적절한 기록을 유지하는 것이 바람직

▶ DSAR 대응 시 정보주체의 모든 관련 정보를 찾는 데 가장 많은 시간이 소요되므로, 컨트롤러는 처리 정보와 개인정보가 저장되는 위치를 쉽게 확인할 수 있는 절차를 확립하는 것이 바람직

- 이를 위해 개인정보 흐름 매핑과 인벤토리 등을 활용할 수 있음

(2) DSAR 제공 정보(GDPR 제15조에 대한 ICO 가이던스[2])

▶ DSAR 대응 시 개인정보 컨트롤러는 정보주체에게 다음의 정보를 제공해야 함

- 처리의 목적
- 관련된 개인정보의 범주
- 개인정보가 공개되었거나 공개될 수신자(또는 수신자 범주)
- 개인정보가 보존되는 기간(또는 보존 기간 결정 기준)
- 컨트롤러에게 개인정보를 수정 또는 삭제하거나 처리를 제한하도록 요청하거나 처리에 이의를 제기할 수 있는 정보주체의 권리

2) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

- 감독기구에 민원을 제기할 수 있는 개인정보 주체의 권리
- 개인정보가 정보 주체로부터 직접 수집되지 않은 경우, 해당 소스에 대한 사용 가능한 모든 정보
- 프로파일링, 로직에 관한 유의미한 정보 및 개인정보 처리로 인해 정보주체에게 초래될 결과 등을 포함한 자동화 의사결정과 관련된 내용

(3) DSAR 공개 보류 정보(개인정보보호법(DPA) 2018[3])

▶ 영국 개인정보보호법(이하 'DPA 2018') 하에서는 컨트롤러가 다음의 목적을 달성하기 위해 접근권을 전체 또는 부분적으로 제한할 수 있다고 명시(제45절(4))

- 공무 또는 법적 탐문, 조사 또는 절차 등을 방해 방지
- 형사 범죄의 예방, 적발, 수사 또는 기소 또는 형사처벌 집행상의 예단 방지
- 공공 안전 보호
- 국가 안보 보호
- 타인의 권리와 자유 보호

▶ 상기의 제한 조건 중에서는 '타인의 권리와 자유 보호'를 위해 정보 공개를 보류하는 경우가 가장 보편적

- 즉, DSAR이 다른 정보주체의 개인정보를 공개해야 하는 경우라면 컨트롤러는 DSAR을 준수할 필요가 없음
- 단, 상대방 정보주체가 정보 공개에 동의한 경우나 해당 공개 행위가 DSAR을 준수하는 것으로 합리적으로 여겨질 때는 예외

▶ 개인정보를 공개하지 않기로 결정한 경우, 해당 정보를 공개하지 않은 이유를 기록하고 적절한 기간 내에 DSAR 정보공개 요청자에게 이를 전달해야 함(ICO 가이던스[4])

3) https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
4) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

(4) 과도한 요청과 합리적인 행정 비용

▶ 영국 정부는 데이터개혁법(Data Reform Bill) 개정안[5]을 통해 컨트롤러가 합리적인 수수료를 부과하거나 요청에 대한 조치를 거부할 수 있는 조치를 완화할 계획(데이터개혁법안 제1편의7)

- 데이터개혁법 개정안에서는 DSAR이 '명백히 불합리하거나 과도한(manifestly unfounded or excessive)'이라는 문구를 '성가시거나 과도한(vexatious or excessive)'으로 변경함으로써, 반복적이거나 악의적으로 발생되는 DSAR에 대해 컨트롤러의 거부를 보다 용이하게 할 수 있도록 조치

※ UK GDPR 하에서의 DSAR 규정 조건은 데이터개혁법안이 최종 통과될 경우 확정될 예정. 동 법안의 제7항(paragraph)은 UK GDPR의 제12조A 규정을 신설토록 하여 개인정보 컨트롤러에게 DSAR 요구가 성가시거나 과도한 경우 DSAR 대응 거부나 비용 부과를 허용

표1 _ 영국 데이터개혁법안: DSAR이 '성가시거나 과도함' 판단 근거(UK GDPR 제12조A)와 사례

고려 사항	사례
• 요구의 성격 • 정보주체와 컨트롤러 간의 관계 • 컨트롤러의 대응 가용 자원 • 데이터 주체가 컨트롤러에 대해 이전의 정보 요청을 반복하는 정도 • 이전 정보 요청이 얼마나 오래전에 이뤄졌는지 정도 • 컨트롤러에 대한 정보주체의 요청이 여타 요청과 중복되는지 여부	• 번거로움을 유발할 의도가 있는 경우 • 신의에 입각하지 않은 경우 • 절차의 남용인 경우

출처: 영국 데이터개혁법안('22.7.18.), 넥스텔리전스 재구성

- 그러나, 요청의 성가심과 과도함 여부를 입증하는 것은 컨트롤러의 몫이므로, 적절한 기록 보관은 필수

- 수수료 규모는 관련 정보 제공에 따른 행정 비용을 기준으로 책정

5) '22.7.18 개정안 발표. UK GDPR의 신설 제12조A 규정. '22.10월 말 현재 하원 2차 독회 통과

3. DSAR 대응 절차와 소통

(1) DSAR 절차 개시

▶ GDPR과 데이터개혁법안 등에 근거하여 정보주체는 접근권을 쉬운 방식과* 합리적인 간격으로 행사할 수 있어야 하며, 서면으로 요청할 필요는 없음

* (GDPR 제12조제1항) 컨트롤러는 "일체의 통지를 정확하고, 투명하며, 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여 정보주체에게 제공하기 위한 적절한 조치를 취해야 하고, 특히 아동을 특정 대상으로 할 때 더욱 그러해야 한다. 해당 정보는 서면이나 적절한 경우, 전자수단 등 기타 수단을 이용하여 제공되어야 한다."

- 정보주체는 조직의 누구에게나 요청을 할 수 있으므로, 모든 직원이 DSAR을 수신할 때 해당 수신 요청 건의 중요성을 인지토록 해야 함
- 따라서 조직 내 모든 직원이 준수할 수 있는 적절한 절차를 마련하는 것이 중요

(2) 영국 DSAR 민원 제기 현황과 대응 권고안

▶ 영국 ICO는 '22.9월 DSAR 준수 관련 문제 대응을 돕기 위한 권고문을 ICO 웹사이트를 통해 공개[6)]

- ICO는 최근 시민들로부터 접수한 민원 사항을 분석한 결과, 개인정보 접근 요청(DSAR)에서 발생되는 공통적인 특징을 확인
  - 일반적으로 DSAR 대응 시간 지체, 만족스럽지 못한 수준의 정보 완결성, 정보 요청 사항에 대한 이해 부족 등이 주요 민원 사항으로 언급

표2 _ 영국 DSAR 민원 원인 유형 및 내용

민원 원인 유형	주요 내용
지연	정보 권리 요청 시 시간이 많이 소요
관계 해체	연락처 부재, 질의에 대한 회신 부재, 불완전하거나 만족스럽지 못한 답변
신뢰	전해 들은 내용에 대한 신뢰 부재
이해	이해 부족으로 인해 접한 정보가 불명확하거나 유용하지 않은 것으로 인지

출처: ICO('22.9), 넥스텔리전스 재구성

6) ICO, Subject Access Requests: Getting the basics right, 2022.9.26

• 이에 따라, ICO는 DSAR에 대한 조직들의 원활한 대응 지원을 위해 ▲시민과의 소통 유지 ▲신뢰 구축을 위한 적극적 응대 ▲프라이버시 정책의 최신성과 접근성 등 다수의 개선 권고 사항을 제시

표3 _ 영국 ICO의 DSAR 문제 해결 대책 가이드

해결 대책	주요 내용
고객과의 소통	• 고객이 원하는 사항을 확인할 것 • 고객의 DSAR 마감일을 맞출 수 없을 경우, 미리 고지할 것
대화가 핵심 관건	• 고객이 구체적으로 필요한 사항을 확인할 것: 대부분의 요청자들은 모든 정보를 요구하나 실제 특정 사안과 관련된 정보만으로도 필요가 해소되는 경우가 빈번 • 요청자의 요청 정보 탐색을 지원하기 위해 정보 처리 상황이나 날짜 등 추가적인 정보를 제공할 수 있는지 요청
선제적 대응으로 신뢰 구축	• 개인정보보호 민원 처리 진행 상황을 모를 때 ICO에 문의하는 경우가 빈번 • 따라서, 복잡하거나 특히 대규모의 DSAR을 다루는 경우 정보를 특정 시간 단위의 정보를 일괄 전송한다는 점을 설명 • 옵트아웃 요청은 즉각적으로 실행되기는 어렵다는 점을 설명 • 예외 적용 사항에 대해 설명할 것: 고객을 충분히 만족시킬 수는 없으나, 특정 경우에 정보가 제공되지 않은 상황이 있다면, 이에 대한 설명을 제공함으로써 고객 민원을 해소할 수 있음
쉬운 언어를 사용	• 개인정보보호 법률의 어휘들은 일반인에게 어려울 수 있으므로, 가급적 이해하기 쉬운 어휘와 문장으로 설명할 것
정직이 최선	• 고객은 자신의 정보가 예상하지 못했던 방식으로 사용되고 있거나 이해하지 못할 때 민원을 제기 • 개인정보보호 방침을 최신 상태로 유지하고 쉽게 액세스하고 이해하기 쉽도록 할 것 • 고객의 입장에서 열린 마음으로 설명할 것

출처: ICO('22.9), 넥스텔리전스 재구성

4. 영국 ICO의 DSAR 관련 최근 동향

(1) ICO의 DSAR 위반 조직 행정 조치 현황과 사례

▶ ICO는 '22.9월 말 정부 부처가 보유한 개인정보에 대한 DSAR 규정 의무를 위반한 7개 조직에 대해 행정 조치를 실시[7]

- DSAR에 대한 대응은 1~3개월 이내에 이뤄지는 것을 원칙(GDPR 제12조제3항)으로 하나 최근 ICO의 조사에서는 공공 및 민간의 7개 조직이 법률적으로 정해진 대응 기간 내에 처리를 하지 못한 것으로 확인

- 이에 따라 ICO는 계고문(reprimand) 발부와 정보자유법(Freedom of Information Act(FOIA) 2000)* 하에 실행 권고안(practice recommendations) 등의 규제 조치를 단행

* '00년에 제정된 법으로 동 법에 시행에 의해 공공기관(public auhthorities)이 보유하는 각종 정보에 대한 공개청구 가능

표 _ 영국 7개 조직의 DSAR 위반 사례 주요 내용

조직		주요 내용
정부	국방부 (Ministry of Defence, MoD)	• '20.3월까지 DSAR가 미처리된 것으로 확인됨에 따라 계고장(reprimand)이 발부됨 • 이후 복구 계획이 마련되고 나서도 미결 건수는 지속적으로 늘어나고 있으며, 현재 9,000건가량이 미결된 상황 • 즉, 정보주체들의 국방부 대상 개인정보 활용 상황 열람 요청 시 정보 수령까지 통상 12개월 이상이 소요
	내무부 (Home Office)	• '21.3월~'21.11월 간 조사 결과 21,000건에 대해 대응이 이뤄지지 않는 등 심각한 지체가 확인되어 계고장 발부 • 내무부로부터 DSAR 회신을 받지 못한 정보주체들은 ICO에 연락하여 쌓인 민원을 토로 • '22.7월 시점 법적 처리 기간 내에 미결된 DSAR는 3,000건이 넘게 남아 있음
	런던 크로이던 버로우 (London Borough of Croydon)	• '20.4월~'21.4월 간 조사 결과 런던 크로이던 버로우 당국은 UK GDPR에서 지정한 기준 대응 시간 이내에 DSAR를 처리한 건수가 절반에 미치지 못한 것으로 나타남 • 당시 미처리 DSAR 건수는 115건으로 나타났으며, ICO는 '21.6월 시점 DSAR 대응 실패와 관련하여 정보자유법(FOIA) 하에서 27개 결정문(decision notices)을 발행 • 이외에도 계고문과 함께 법적 대응 기간 충족에 실패한 FOI 규제에 대해 새로운 접근법 하에서 실행 권고안(practice recommendation) 발부

7) ICO, Action taken against SEVEN organisations who failed in their duty to respond to information access requests, 2022.9.28

조직		주요 내용
	켄트 경찰청 (Kent Police)	• '20.10월~'21.2월 사이 켄트 경찰청은 200개 이상의 DSAR을 접수했으며, 이 중 60%를 법정 기일 내에 회신 • 그러나 나머지 DSAR은 대응까지 18개월 이상이 소요되는 경우도 발생 • '22.5월 시점 200개 이상의 DSAR가 미결된 상황으로 계고장 발부
민간	버진 미디어 (Virgin Media)	• '21.7월~12월 기간동안 Virgin Media(통신 미디어 기업)는 9,500개 이상의 DSAR를 수령 • 이 중 1,316건(14%)은 법정 대응 기간 내에 미회신 • 이후 '22년에는 DSAR 회신 관행에 진전을 보였으나 여전히 만족스러운 수준에 도달하는 데 실패하여 ICO는 '22.9월 계고장 발부

출처: ICO('22.9), 넥스텔리전스 재구성

(2) ICO 공공 자문 결과: DSAR 악용 조직 대응책

▶ 디지털문화미디어스포츠부(DCMS)는 '21.9월 DSAR에 대한 비용 부과와 DSAR에 대한 개인정보 컨트롤러의 거절 권리 허용과 관련된 공공 자문[8]을 실시

- DCMS는 EU 탈퇴와 함께 자체적인 개인정보보호 법률 프레임워크 수립의 일환으로 기업에 대한 부담 감소와 시민들에 보다 나은 행정 결과물 제공을 목표로 DSAR에 대한 개정 방안을 검토

- 개정 방안에는 i) DSAR 요청 시 별도 비용을 부과하는 방안을 재도입할지 여부와 ii) 명백히 불합리하고 과도한 조건(on the basis of it being manifestly unfounded and excessive) 하에서 DSAR 거부권 행사를 허용하는 현행 규정 변경* 여부 등이 포함

  * 데이터개혁법안 하 컨트롤러의 거부 조건 관련 문구(vexatious or excessive)로의 변경

▶ DCMS는 '22.6월 약 3,000개에 달하는 자문 의견을 수렴하여 이에 대한 대응 문서[9]를 발간하며 다음과 같이 결론을 내림

- 정부는 정보주체의 DSAR에 대한 별도 비용을 부과하지 않을 계획

8) DCMS, Data: A new direction, 2021.9.10
9) DCMS, Consultation outcome- Data: a new direction - government response to consultation, 2022.6.23

- 정부는 데이터개혁법안 통과 시, DSAR 거부권 행사를 허용하는 현행 규정의 단서 문구인 '명백히 불합리하거나 과도한(manifestly unfounded or excessive)'을 '성가시거나 과도한(vexatious or excessive)'으로 수정할 계획

5. 시사점

▶ **(개정법, 정보주체의 DSAR 남용 견제)** 영국은 정보주체의 DSAR 남용이 문제가 되고 있는 가운데, 데이터개혁법안이 확정될 경우, DSAR 거부권 행사를 위해 새롭게 삽입된 문구인 '성가신'에 대해 ICO와 법원이 내리게 될 해석에 귀추가 주목

- 만약 ICO가 해당 문구에 대한 정의를 폭넓게 해석할 경우, 컨트롤러와의 법률 분쟁수단으로 DSAR을 남용해 온 정보주체들에게는 불리하게 법률 적용이 이뤄질 것으로 예상

- 이에 대해 정보주체들의 변호인단은 DSAR을 개별 분쟁 단위의 별건으로 진행함으로써 개인정보 처리에 대한 우려를 구체적으로 부각시키는 전략을 채택하며 컨트롤러를 압박할 가능성도 배제할 수 없음[10)]

- 그럼에도 불구하고, 데이터개혁법안이 현재안대로 확정될 경우, 개인정보 주체-컨트롤러 간 법률 분쟁 시 악의적이고 반복적인 DSAR을 통해 컨트롤러에 법률적인 부담을 가중시켜 온 관행을 방지하는 데는 상당한 효과를 낼 수 있을 것으로 기대

▶ **(국내 정보주체의 권리 행사 촉진)** 영국 등 GDPR의 영향력 하에 있는 유럽 국가들에 비해 우리나라는 정보주체의 권리 행사가 제한적이며, 이를 해소하기 위한 제도 환기 및 법제 보완이 요청됨

- 국내에서는 개인정보보호법 하에서 개인정보의 열람(제35조), 정정삭제(제36조), 처리 정지(제37조), 권리 해사의 방법 및 절차(제38조) 등을 통해 정보주체의 권리를 보장

- 그러나 개인정보보호법상에서의 정보주체 권리 행사에 대한 인지도 부족 및 절차적인 복잡성과 함께 권리행사를 보장하고 실행할 수 있도록 하기 위한 법 규범의 미비로 정보주체의 권리 행사는 활발하게 이뤄지지 않고 있는 상황

10) Osborne Clarke, UK government proposes clamp down on use of data subject access requests as a litigation tactic, 2022.8.5.

- 일례로, 개인정보보호법 시행령에 따르면 정보주체가 개인정보 열람을 요구하려면 개인정보처리자가 마련한 방법과 절차에 따를 것을 요구할 것을 의무화(제41조)
- 이에 반해, GDPR에서는 DSAR 요청을 위한 별도의 요구사항을 규정하지 않고 있으며, ICO 역시 별도의 신청 양식이나 연락처 등을 특정하지 않으며 제3자를 통해서도 이를 가능케 하는 등 정보주체 측면의 DSAR 자유도를 적극적으로 보장
- 따라서, 개인정보 열람 절차의 간소화를 위한 법제 정비와 정보주체 권리 행사를 제대로 할 수 있도록 정부 차원의 노력 필요

Reference

1. DCMS, Consultation outcome- Data: a new direction - government response to consultation, 2022.6.23
2. DCMS, Data: A new direction, 2021.9.100
3. ICO, Action taken against SEVEN organisations who failed in their duty to respond to information access requests, 2022.9.28
4. ICO, Subject Access Requests: Getting the basics right, 2022.9.26
5. ICO, Subject Access Requests: A Data Controller's Guide, 2022.10.5
6. Osborne Clarke, UK government proposes clamp down on use of data subject access requests as a litigation tactic, 2022.

드론 이용 확산에 따른 개인정보보호 이슈 분석

[목 차]

1. 배경

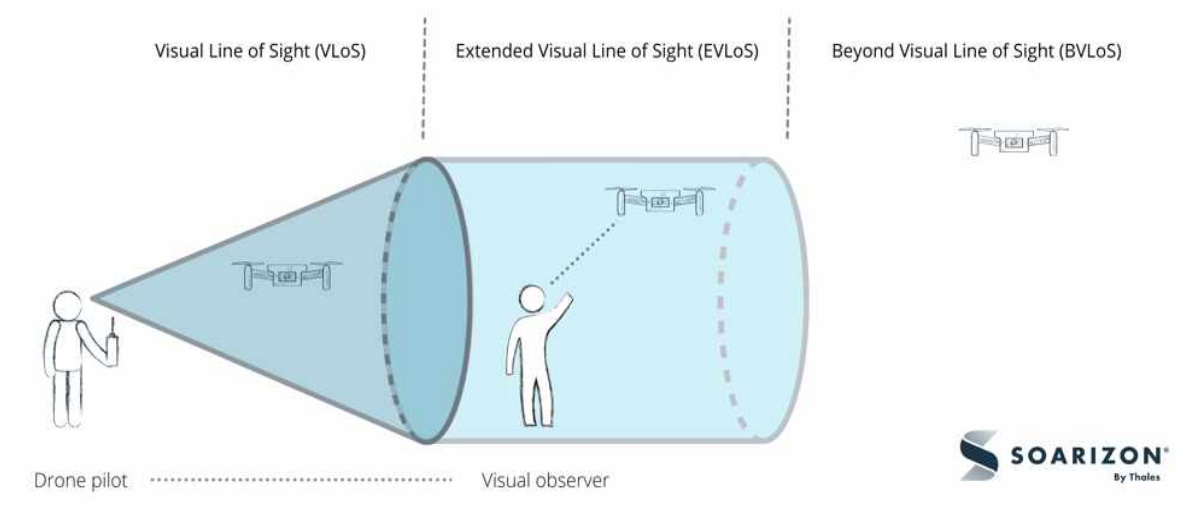
▶ 전 세계적으로 드론 이용의 빠른 확산과 기술의 발전으로 사생활 및 개인정보 침해 우려가 크게 증대되는 가운데, 미국과 EU를 중심으로 새로운 규제 도입 및 적용에 대한 논의가 본격화됨[11)]

- 미국은 연방항공청(Federal Aviation Administration, FAA)을 중심으로 非가시권 드론(BVLOS)*에 대한 새로운 규제 도입을 준비 중이며, 이를 통해 관련 산업 육성과 드론 이용 효율성을 높이려는 정책을 추진

11) 국내는 2021년 들어 드론 분류체계를 개편하고, 기체 신고의무와 조종자격 강화를 담은 법안(항공안전법 시행령, 항공안전법 시행규칙)이 시행됐고, 드론 안전확보와 사생활 침해에 대한 처벌 규정 마련이 필요하다는 의견이 제기

* Beyond Visual Line of Sight(BVLOS) 드론 : 조종자 시야 범위를 벗어난 非가시권 드론을 의미, 이와 비교되는 개념으로 조종자가 육안으로 드론을 확인할 수 있는 Visual Line of Sight(VLOS, 가시권) 드론, 관찰자를 통해 가시권을 확장한 Extended Visual Line of Sight(EVLOS, 확장가시권) 드론이 있음

그림 _ VLOS, EVLOS, BVLOS 비교



출처: ScaleFlyt(https://www.scaleflyt.com/news/what-are-vlos-evlos-and-bvlos-why-do-they-affect-drone-operations)

- EU는 드론으로 인한 시민의 자유 및 개인정보 침해 방지에 주력하고 최근 아일랜드 개인정보 감독기구(DPC)가 개인정보 침해에 대한 구분과 규제 적용 관련 백서를 발간

▶ **(미국)** FAA는 2016년 기존 연방 항공규정(Federal Aviation Regulation)에 소형 드론 규제(Part 107*)를 추가했고, 2020년에 드론 식별을 위한 '원격 식별'** 규정을 도입하는 등 적극적인 드론 규제 정비에 나섬

* 연방 항공규정 Part 107(Federal Aviation Regulation Part 107) : 드론에 대한 운행 제한, 원격 조종사 자격, 책임· 비행체 요건 등을 규정해 소형 드론의 운행 안정성을 보장

** Remote ID : 연방 항공규정 Part 89에 추가된 의무로, 등록이 필요한 드론의 경우 원격에서 식별할 수 있도록 신원, 위치, 고도, 이륙 위치 등의 드론 관련 정보 제공을 명시

- 하지만 이는 모두 드론 위치 파악이 가능한 가시권 드론에 국한된다는 지적이 제기

- FAA는 규제에서 벗어나 있는 BVLOS 문제 해결을 위해 BVLOS 드론 항공제도 정비위원회(ARC)*를 소집해 규정 제정에 착수했고, 2022년 3월 그간 성과를 담은 UAS** BVLOS ARC 최종보고서***를 공개

* Aviation Rulemaking Committee(ARC) : 연방 항공규정 개정 시 꼭 거쳐야 하는 규제정비 자문단으로, FAA 내부, 산업계 커뮤니티, 시민단체 동이 참여해 의견을 개진

** Uncrewed Aircraft Systems : 조종사가 없는 무인 항공기를 의미하며, 통상 드론을 지칭하는 용어

*** Advisory and Rulemaking Committees UAS BVLOS ARC Final Report

- BVLOS ARC 최종보고서는 BVLOS 드론의 개인정보보호를 위한 권장사항 등을 담고 있지만, 논의에 참여했던 EFF, ACLU, EPIC 등 시민단체들은 보고서 동의를 거부해 논란

- 시민단체들은 ARC에서 산업계 커뮤니티의 비중이 너무 컸고, 6개월이라는 시간제한으로 드론 개인정보보호에 대한 충분한 논의가 이뤄지지 않은 점 등을 반대 이유로 제시

- FAA는 최종보고서에 시민단체가 제기한 문제들을 부록으로 수록해 논의 가능성을 열어뒀고, EEF 등은 BVLOS 드론 개인정보보호에 대한 권고를 제안하고 있어 논의가 계속 이어질 전망

▶ **(EU)** 아일랜드 DPC는 2022년 6월 드론 사용에 대한 가이던스(Guidance on the Use of Drones)[12]를 발표하고, 개인정보보호에서 드론 사용자와 개인정보 주체 간 권리를 명확화하는 노력을 시도

- DPC는 UAS가 원격으로 각종 센서 등 데이터 수집시스템을 통해 이미지, 비디오, 사운드, 기타 정보를 수집하고, 이를 스마트 장치에 전송하는 과정에서 개인정보 처리가 가능하므로 개인정보 컨트롤러에 해당한다고 규정

- 드론은 모바일을 통해 개인정보를 효율적 수집이 가능하다는 점에서 신체착용카메라(BWC)와 유사하다고 평가하고, 둘 다 EU 개인정보보호 기본원칙* 적용 대상이라 강조

* Data Protection Basics: 비상업적 개인·가정 활동이나 공공의 법 집행과 같은 GDPR 개인정보보호 예외 규정에 대한 개인정보 컨트롤러와 개인정보 주체의 권리 등을 명시

- DPC는 동 드론 가이던스에서 안전·인증 등 세부사항은 다루지 않고, 드론 운영자가 EU 법집행지침(LED)* 준수를 위한 개인정보보호 기준을 명확하게 제시

* Law Enforcement Directive(LED) : 법집행당국의 개인정보 처리에 대한 EU 지침

2. 드론의 개인정보 침해 위협과 유형

(1) BVLOS 드론 확산과 개인정보 침해 위협 증대

▶ 전자프론티어재단(EEF)*과 전자개인정보센터(EPIC)** 등 개인정보 시민단체는 BVLOS 드론이 상업적 장점에도 불구하고, 일상적 대규모 비행으로 개인정보를 크게 위협한다고 진단

* Electronic Frontier Foundation : 1990년 디지털 환경에서 인권 보호를 위해 설립된 글로벌 비영리 기구로 법률적 지원뿐 아니라 출판, 저작권, 기술지원 등 다양한 활동으로 큰 영향력을 확보(www.eff.org)

** Electronic Privacy Information Center : 디지털 환경에서 개인정보, 표현의 자유, 민주적 가치 보호를 목적으로 1994년 워싱턴 DC에 설립된 공익 연구센터

- 드론은 기술 발전으로 점점 더 저렴하고, 더 멀리 날고, 더 다양하고 무거운 감시 장비의 탑재가 가능해졌고, 그 결과 지속시간, 거리, 고도의 운영의 유연성으로 감시 여부를

12) Guidance를 지침으로 번역할 수 있으나, EU 법체계에서 Directive를 지침으로 옮기므로 여기에서는 가이던스로 함

파악하기가 더욱 어려워졌다고 지적

▶ 이미 드론은 고도화된 성능과 데이터 수집시스템 진화로 지상 및 온라인 추적 시스템과 연계할 경우 시민의 신원확인, 위치추적이 가능한 강력한 감시 플랫폼으로 진화

- 대부분 드론은 사진 촬영 및 이미지 저장이 가능한 카메라가 장착되어 있고, 소형 소비자 드론에도 4K 카메라가 사용되고, 군용 드론에는 도시 크기의 지역을 촬영할 수 있는 기가픽셀 카메라가 장착

- 카메라 외에 마이크, 열 및 동작 센서, 휴대전화 차단장치, GPS, 레이더, 라이다(LiDAR), 음파탐지기(sonar), 거리 측정기, 자기장 변화 감지, 무선 주파수 센서 등을 탑재

- 드론 항공 감시는 저렴하게 운영할 수 있을 뿐 아니라. 대다수 소비자용 드론이 특정 지상 물체 추적이나 특정 비행경로 주행이 가능하도록 개발되어 즉시 적용이 가능

- 개인정보가 금전적 가치가 커지고, BVLOS 드론 진입장벽이 계속해서 낮아지면서 항공 개인정보 수집 관행은 더욱 확대될 전망

(2) BVLOS 드론을 통한 감시와 개인정보 침해 가능성 유형

▶ EEF는 BVLOS 드론이 매우 광범위한 영역에서 창의적 활용이 가능해, 이로 인한 개인정보 침해 범주 예측은 별 의미가 없다고 지적하고, 일반적인 우려를 제시

▶ **(사람 식별)** 드론을 생화학 센서 등과 결합하면, 사람 얼굴, 차량 번호판 인식 등이 가능하고, 이를 온라인 감시 기술과 연동하면, 사람과 차량 식별은 물론 시간과 공간에 따른 움직임을 추적하거나 연관성 분석이 가능

- EEF는 BVLOS 드론의 광범위한 개인정보 수집 능력은 대중으로부터 은밀하게 개인정보를 수집할 수 있는 엄청난 기회와 위협이 공존한다는 것을 의미한다고 경고

▶ **(항공감시 위협 증가)** 드론의 상대적으로 낮은 진입장벽과 항공감시에 대한 법적 보호 부재가 개인정보 노출의 위험을 크게 고조시킴

- 현재 드론을 비롯한 공공장소의 항공감시에 관한 법률은 모호한 상태며, 드론의 광범위한 가용성에 비해 대중의 개인정보보호를 위한 법적 장치는 충분한 수준에 도달하지 못함

- 이미 반자율 또는 완전 자율화된 드론 운영이 가능하고 한 사람이 한 번에 여러 드론 비행을 감독하는 기능도 등장

- 특히 자율형 BVLOS 드론 운영은 수동 가시권 드론으로는 할 수 없던 방식으로 광범위한

드론을 통한 감시가 가능해질 전망

▶ **(도시데이터 수집)** 가시광선 또는 적외선 스펙트럼 센서를 이용해 어느 집에 불이 켜졌는지, 난방이 되는지 등을 탐사해 주택 점유율을 조사하거나, 시간대별 주차 자랑의 양과 유형 등을 측정하는 것이 가능해짐

▶ **(고객위치 파악)** 상점이나 레스토랑은 무작위로 선택된 고객을 추적해 고객이 어디에서 왔는지, 돌아가는지를 파악하고, 고객의 개인정보(정원, 뒤뜰 그릴 소유 여부 등)를 파악해 마케팅에 활용하는 것이 가능

▶ **(와이파이 식별)** 아직 등장하지 않은 유형의 개인정보 침해도 등장할 수 있으며, 가령 와이파이 식별기 등을 통해 통신사 정보와 온라인 개인 프로필 연계도 가능할 수 있음

▶ **(원치 않는 사생활 침해)** 개인정보 수집이 없더라도 시민은 공중에 드론이 떠 있다는 사실만으로 불편을 느끼고, 감시 가능성 때문에 사생활이 침해됐다고 느낄 수 있음

- 사생활 침해는 감시 상황 기피, 은둔에 대한 침입, 개인 취향 환경의 파괴, 협박, 소음 등에 대한 불편한 감정 등을 모두 포괄하므로, 드론은 광범위한 사생활 침해를 가져올 수 있음

▶ **(법 집행 부작용)** 법집행기관은 감시나 주적 등 법 집행 과정에서 드론을 통해 수집된 개인정보를 사용할 수 있지만, 이 경우 개인정보 침해 및 남용 가능성에 대한 논란으로 법 집행에서 문제가 발생할 수 있음

3. 미국 : FAA의 UAS BVLOS ARC 최종보고서를 둘러싼 이슈 분석

▶ FAA는 2016년 연방 항공규정에 소형 드론을 추가한 후, 곧바로 BVLOS 드론 규정 마련에 나서 BVLOS 산업 육성과 드론의 효율성 제고를 개시

- BVLOS 커뮤니티와 EEF, EPIC 등 개인정보 관련 시민단체들로 ARC를 구성해 다양한 의견을 수렴했고, 2022년 3월 UAS BVLOS ARC 최종보고서를 발표

- 최종보고서 발표에 앞서 EEF 등 시민단체는 2021년 12월 BVLOS 관련 개인정보보호에 대한 제안을 발표하는 등 ARC 활동에 적극적으로 협력했지만, 최종보고서 발표 후 반대 입장을 밝혀 논란 발생

- BVLOS 드론을 둘러싼 논란을 ▲EEF의 개인정보보호 제안('21.12) ▲FAA ARC 최종보고서 발표('22.03) ▲EEF의 ARC 최종보고서 동의 반대('22.08) 등의 이슈를 시간순으로 검토

(1) EEF, BVLOS 드론을 위한 개인정보보호 고려사항 제안('21.12)

▶ EEF은 2021년 12월 개인정보보호 민간단체 EPIC과 공동으로 FAA의 BVLOS 드론 운영 규제 제정에 대한 BVLOS 드론을 의한 개인정보보호 제안*을 전달

* Privacy Considerations for BVLOS Drones

- EEF는 BVLOS 드론이 배달, 기반 시설 감시, 정밀농업 등에 새로운 기회와 효율을 제공하지만, 동시에 개인정보보호에 심각한 위협으로 작용한다고 지적
- EFF는 FAA와 BVLOS 산업계가 BVLOS 드론 활성화에 앞서 제품의 개인정보보호에 대한 투명성과 명확한 보호 조치에 대한 문제 해결에 나서야 한다고 강조

▶ EFF는 드론을 자율적 비행이나 원격 조종이 가능한 무인 항공기 시스템(UAS)으로 정의하고, 기술 발전 등으로 매우 빠른 확산과 진화가 전개되고 있다고 평가

- 지난 몇 년 동안 드론은 비디오·사진 애호가들 사이에서 큰 화제가 됐고, 거액의 상금을 놓고 150개 팀이 참여한 드론 레이싱(World Drone Prix) 경주가 개최되는 등 저변이 크게 확산됐다고 평가
- 특히 BVLOS 드론은 조종자 시야에서 벗어나 지평선 너머나 혹은 지구 반대편에 있을 수 있을 만큼 진화해 드론의 통신 제어, 주변공간에 대한 인식 등에서 훨씬 정교한 규정이 필요하다고 강조
- 현재 BVLOS 드론은 관련 규정이 없어 BVLOS 드론 운행을 위해서는 FAA에 규정 면제를 신청해야 하는 등 규제 사각지대에 위치해 있다고 설명
- EEF는 BVLOS 업계가 상업적 배달 등 장거리 드론의 상업적 활용에 집중해, 각종 개인정보 수집이 가능한 센서를 탑재한 드론이 운행 중이며, 이를 통해 차량 소유 여부, 차 번호, 주차 시간, 소유자 얼굴 등의 개인정보 수집과 유출이 우려되는 상황이라고 경고

(2) FAA, UAS BVLOS ARC 최종보고서 발표('22.03)

▶ **(배경)** FAA는 상용 UAS는 안전과 효율성이 중요하다고 강조하고, 상용 드론이 의약품 운송 등에 활용되면서, 미국인에게 큰 공공 혜택과 서비스를 제공하고 있다고 평가

- FAA는 드론의 활용 증가에도 불구하고, 활용도가 더욱 높은 BVLOS 관련 규제가 존재하지 않아 드론 활성화와 산업 육성에 부정적 영향을 미친다고 진단
- 현행 규제는 고도로 자동화된 드론을 안전하게 운용하는 데 충분하지 않으며, BVLOS 드론에 확장 적용하는 것 역시 부적절하다고 평가해 새 규제 도입을 추진

▶ **(목적)** BVLOS에 대한 새로운 규제 프레임워크는 안전이 보장된 드론 활용 촉진과 지속가능한 운송 솔루션 확보를 통한 항공 혁신에서 미국의 리더십 보장이라고 강조

- BVLOS 규제 제정은 기존 규제에 BVLOS 장점을 안전하게 극대화하는 방향으로 통합을 목표로 하며, ARC를 통해 각종 리소스·기술·전문지식을 반영할 방침이라고 천명

▶ **(과정)** FAA는 2016년 6월 '소형 무인 항공기 시스템의 운영 및 인증'에 대한 연방 규정 코드를 제정해 국가 공역시스템(NAS)*에서의 드론 운영에 대한 요구사항 명시

* National Airspace System: 미국의 영공, 항법 시설, 공항과 관련 정보, 서비스, 규칙, 규정, 정책, 절차, 인력, 장비들을 아우르는 항공 시스템

- 하지만 동 규정은 드론 설계·제조·생산에 대한 요구사항을 전혀 포함하지 않았고, 대신 드론 운영에 대한 특정 지역(G등급 공역*에서는 400ft(120m) 이하 비행) 및 조건(식별이 가능한 지역 내 비행)과 같은 항공기의 운항 안전과 지상 시민의 재산권 보호만을 규정

* G Class Airspace: 항공교통관제업무가 제공되지 않는 비관제지역으로 미국의 경우 공항지역은 지상고도(AGL) 700ft, 항로지역이면 1,200ft 이내 높이의 공역이 해당

- 당시 FAA는 동 규정이 미국에서 저위험 VLOS(가시권) 드론 운영을 위한 중요한 조치였다고 평가했고, 지금은 활용 증가세에 있는 BVLOS 드론에 대한 새로운 논의가 필요하다고 강조

표1 _ ARC 최종보고서 주요 권고사항 내용

권고사항	주요 내용
공역 및 지상 위험 권고	• FAA가 수행하는 모든 유형의 작업에서 일관되게 드론에 대하여 허용 가능한 위험 수준(Acceptable Level of Risk, ALR) 설정 권고 - FAA는 해당 권고를 수용하여 드론 운영자에게 공통적이고 일관된 규정 및 지침을 채택해 정성적 또는 정량적, 혹은 이 둘을 결합한 하이브리드 접근 방식을 통해 ALR을 제시할 방침
비행권 규칙 권고	• 주요 구조물 및 기반 시설 100ft 이내와 400ft 미만으로 규정된 저고도 보호지역(Low Altitude Shielded Areas)과 저고도 비보호지역(Low Altitude Non-Shielded Areas) 규정(42 U.S.Code § 5195c - Critical infrastructures protection)[13] 수정 권고 • 드론 운영 활성화를 위해 저고도 보호지역에서 위성항법장치(ADS-B)가 장착되지 않은 드론에 비행 우선권 부여 등을 권고
조종사 자격 관련 권고	• 소형 드론의 원격 조종사 인증 규정을 담고 있는 파트 107의 적용범위를 확대해 가시권을 확장한 EVLOS 드론이나 차폐가 되어 있는 UAS와 같은 제한적인 BVLOS 드론을 포함하기를 권고 - 해당 권고는 기존 Part 107 규정을 넘어 새로운 원격 조종사 인증이 등장한다는 의미로, 두 등급 인증에 대한 세부적인 조정 과정이 필요하다고 지적
새로운 규정 파트 신설 권고	• 새로운 규정인 파트 108 제정 권고 • 동 규정은 최대 출력 800,000 ft-lb(피트파운드력[14]) BVLOS 드론에 적용하는 것에 기반하며, 이에 따라 새로운 자격 인증 프로세스 개발이 필요
제3자 서비스 규제 관련 권고	• BVLOS 드론 운영을 지원하는 제3자 서비스에 대해 비의무 방식의 규제체계를 마련할 것을 권고

출처: Wiley, FAA Committee Releases BVLOS Recommendations, 2022.3.14.

▶ FAA는 ARC 최종보고서는 UAS BVLOS 운영과 관련한 안전, 경제성, 환경적 가치 등을 고려한 UAS 파일럿 프로그램(Integration Pilot Program, IPS)과 안전 계획 수립을 위한 파트너십(Partnership for Safety Plans, PSPs) 등의 프로젝트를 통해 도출한 UAS BVLOS 최소 성능 기준이라고 강조

- FAA는 UAS BVLOS ARC 보고서가 공역에서 안전하고, 확장 가능하고, 경제적이며, 친환경적인 UAS BVLOS 운영을 위한 기준으로 개발된 결과물이라고 평가

(3) EEF, FAA의 UAS BVLOS ARC 최종보고서 동의 반대('22.08)

▶ EFF는 FAA가 ARC에서 개인정보보호 시민단체의 참여와 의견 청취를 요청한 것은 긍정적이지만, 시민 자유 위협에 대한 논의 공간으로서 ARC 역할은 미흡했다고 지적

- EEF는 ARC 보고서에 대해 ▲자발적 개인정보보호 관행은 구속력이 없어 남용 가능 ▲드론의 정보 및 운행 목적에 대해 투명성 부족 ▲개인정보 침해 영향에 대해 고려 부족 ▲드론의 부정적 사용 및 영향에 대한 고려 부족 등을 지적하며 반대 의사를 표명

- EFF는 ARC 보고서에 대한 반대의견 제시에 그치지 않고 FAA의 역할에 대해서도 2021년 12월 발표한 'BVLOS 드론을 위한 개인정보보호 고려사항' 백서*의 내용을 참고할 것을 제시

* EFF, Privacy Considerations for BVLOS Drones: Privacy Considerations for FAA Aviation Rulemaking Committee on Beyond Visual Line of Sight Drone Flights, 2021.12.

BVLOS 드론을 위한 개인정보보호 고려사항('21.12)

▶ **(개인정보보호에서 FAA 역할)** EFF는 FAA가 국가 공역의 드론 통합 관리를 위해서는 개인정보보호 문제 해결을 바탕으로 한 대중적 수용이 필요하다고 강조

- EFF는 FAA가 드론을 통합 감독하는 기관으로서 개인정보 위협 해결과 새로운 위협에 대한 문제 해결 프로세스 설정에 집중해 줄 것을 요청
- 또한 FAA가 개인정보보호 프로세스를 ▲투명성 ▲지방정부 자율 보장 ▲원격 ID 활용 등을 핵심 요소로 삼을 것을 제안

▶ **(투명성)** 시민이 BVLOS 드론을 수용하기 위한 가장 기본적 요소로, 대중과 기관이 BVLOS 운영자에게 책임을 묻고, 시민의 권리를 행사할 수 있도록 구현해야 함

- BVLOS 운영자는 드론 운영이 국가 공역시스템(NAS)과 지상에 있는 사람들에게 미치는 영향(안전, 소음, 환경 등)을 파악하고, 사생활에 미치는 영향을 평가해야 함

13) 동 법률의 약칭은 "Critical infrastructures protection Act of 2001"임
https://www.govinfo.gov/app/details/USCODE-2010-title42/USCODE-2010-title42-chap68-subchapIV-B-sec5195c/summary
14) 1중량 파운드의 힘이 가해지는 방향으로 물체를 1피트 움직일 때의 일 또는 에너지의 단위

- 영향평가는 대중이 쉽게 활용할 수 있도록 해야 하고, 드론 종류와 목적, 운영 목적, 기술 능력(탑재 센서, 센서의 능력, 개인정보 수집 능력 등) 등의 세부 정보를 포함해야 함

▶ **(지방정부 자율성 보장)** FAA는 개인정보보호 또는 기타 가치를 보호하고 지역 혁신을 장려하기 위해 지방정부 및 기관에 자체 규칙 설정을 허용해야 한다고 제안

- 드론 운영 규칙 적용은 지방 정부에 맡기고 FAA는 개인이 개인정보 관련 우려와 민원을 제기하고, 드론으로부터 경험한 소음 및 안전 문제 등을 비롯한 개인정보 침해 경험을 보고할 수 있는 메커니즘 구축에 집중해야 함

▶ **(원격 ID 개선)** 원격 ID 요구사항은 드론의 대중적 수용과 함께 개인정보보호 관련 규정을 구현할 좋은 기회라고 강조

- 원격 ID는 드론의 행로, 감시능력, 용도, 수집할 수 있는 정보 등의 추가 정보를 대중이 알 수 있도록 해 드론에 절실한 투명성을 촉진할 수 있음
- 이런 이유로 원격 ID 요구사항은 복잡하지 않고 대중이 유용하게 사용할 수 있게 구현하는 것이 중요하며, 데이터베이스에 접속해 드론 정보를 쉽게 파악할 수 있어야 한다고 강조
- 원격 ID는 지상에 있는 사람이 공중에 떠 있는 BVLOS 드론에 대한 주요 정보를 얻을 수 있는 프로그램을 구현하되, 전국의 모든 드론 비행을 추적하는 시스템 구현 시도는 부적절함

▶ **(기타 추가사항)** 의회는 정부 및 상업 BVLOS 운영자에게 운영에 필요한 개인정보 수집·사용·공유 최소화를 요구하고, 특정 목적으로 수집한 개인정보는 타목적으로 사용할 수 없도록 해야 함

- 예를 들어 배송을 위한 드론은 배송 목적에 필요하지 않은 개인정보는 수집할 수 없으며, 해당 배송 목적 외에 수집된 정보는 매핑 서비스 등의 목적에 사용해서는 안 됨
- 개인정보 수집·사용·공유 최소화를 위한 의무사항에는 기술적 사용도 포함할 것. 예를 들어 철도의 안전 평가를 수행하는 드론은 주변 주택의 정원을 촬영하는 것을 전자적으로 차단

4. EU : 아일랜드 DPC의 드론 이용 백서에서의 개인정보보호 이슈 분석

(1) 개인정보 컨트롤러와 개인정보보호 의무

▶ DPC는 드론으로 통칭하는 UAS를 원격으로 이미지, 비디오, 사운드 또는 기타 정보를 수집(데이터 수집시스템)해 이를 스마트 디바이스(클라우드 스토리지)로 전송하는 기능을 갖춘 다양한 크기의 광범위한 항공기 범주로 규정

▶ **(개인정보 컨트롤러)** EU는 '개인정보보호 기본원칙'에서 드론은 장착된 개인정보 수집 시스템을 통해 식별 가능한 개인정보를 수집하기 때문에 개인정보 컨트롤러에 해당하며, 동시에 개인정보보호법 준수 의무가 있다고 규정

- 가령, 드론에 카메라가 장착되어 있고 카메라를 작동해 개인을 식별할 수 있는 높이에서 비디오 또는 사진을 촬영할 경우, 툴(tool)을 이용해 확대·축소와 같은 개인정보 처리가 가능하고 개인 이미지 촬영을 결정했기 때문에 개인정보 컨트롤러가 된다고 설명

- 개인정보 컨트롤러는 드론 촬영이 ▲대상자의 이익을 위한 것 ▲목적 달성에 필요한 것 ▲개인에게 불균형적인 영향을 미치지 않는 점 등을 입증해야 적법성을 확보할 수 있음

▶ **(개인정보보호 의무)** 개인정보 컨트롤러는 드론 작동 전에 규정 준수 여부를 확인해야 하고, 언제든지 DPC에 규정 준수를 입증할 수 있어야 한다는 책임 의무를 가짐

- 합법적인 개인정보 처리 활동을 위해 개인정보보호법뿐 아니라 무단 침입에 대한 관한 불법 행위법, 항공법 등 관련 법률을 준수해야 함

- 드론으로 개인정보를 수집하는 목적을 분명히 하고 최종적으로 제3자에게 개인정보 공개 등의 개인정보 처리는 법적 근거를 따라야 한다고 명시

- 꼭 필요한 경우에만 개인정보를 수집·사용하고, 이 경우 개인정보를 최소화해야 하며, 이를 기반으로 개인정보 수집 시스템과 개인정보 저장 시스템을 설정해야 한다고 명시

▶ **(드론 구매)** 드론 소유자는 개인정보 컨트롤러로서 드론의 설계 및 기능이 개인정보 보호를 준수하는지를 확인해야 하는 책임을 지님

- 또 영상 저장 장소가 장치 자체인지, 클라우드 스토리지인지 등을 확인하고 개인정보의 추가 손실 또는 도난 위험을 완화하기 위한 조치 역시 모두 소유자 책임으로 규정

▶ **(제3자 서비스)** 드론으로 수집한 개인정보가 클라우드 서비스와 같은 제3자 서비스를 이용할 경우, 드론 소유자는 개인정보 컨트롤러로서 개인정보보호법의 주요 책임을 짐

- 가령, 제3자 클라우드 서비스가 유럽경제지역(EEA) 외부에 있을 경우, 아직 해당국의 개인정보보호법에 대한 EU 집행위원회의 적정성 결정이 없다면, 개인정보의 해외 전송에 대한 책임은 드론 소유자가 져야 함

▶ **(개인정보 컨트롤러 정보제공)** 개인정보보호 관련 DPC 결정에 이의 제기를 위해서는 먼저 개인정보 컨트롤러의 세부 정보를 제공해야 함

(2) 개인정보보호 예외 규정과 위반 사례

▶ DPC는 드론 이용 백서에서 드론 개인정보보호 위반 사례와 각종 예외 규정을 제시해 드론 사용자의 이해를 도움

- DPC는 GDPR에 규정되지 않았거나, 기존 법과 충돌하는 상황 등을 사례로 설명

▶ (유형1 : 컨트롤러 인정) 카메라가 장착된 드론을 이용해 개인을 식별할 수 있는 높이에서 비디오 또는 사진을 촬영할 경우, 드론 사용자는 개인정보 컨트롤러에 해당

- 드론을 통해 확보한 사진을 툴을 이용해 확대·축소 등의 개인정보 처리가 가능하고, 개인 사진 촬영을 결정했기 때문이라고 설명

▶ (유형 2 : 컨트롤러 예외) 취미가 사진 촬영이고 공원에서 새로 구입한 드론을 시험 비행한 사람의 경우, 컨트롤러에 해당하지만, 감시활동에 해당하지 않고 촬영 사진을 외부에 공개하지 않는 경우 개인적 활동으로 인정

▶ (유형 3 : 감시목적 사용금지) GDPR은 공개 장소에서 사진 촬영을 금지하지 않지만, 광장 감시 목적으로 드론을 비행시키고 이때 드론이 사진을 촬영했다면 이는 개인 및 가정 활동으로 간주되지 않으며, 개인정보 침해 문제가 발생

- 하지만 드론이 아주 높은 고도에서 자신 소유 건물 사진만 촬영했다면 이는 개인정보보호 규정이 적용되지 않으며, 이런 상황은 건물에 설치된 CCTV에도 동일하게 적용

▶ (유형 4 : 영상 공개) 드론 촬영 목적이 상해 발생 시 비용청구를 위한 것이라면, 소송에서 관련 영상을 변호사에 공개하는 것은 촬영 목적과 공개 행위가 일치하므로 합법

- 반면, 이 영상을 교육용이나 기타 목적으로 일반인에게 공개하는 것은 목적이 일치하지 않기 때문에 공개할 경우 처벌 대상이 됨

▶ (유형 5 : 합법적 논리 허용) 드론 영상의 개인정보 처리는 동의를 기반으로 하지만, 특정 상황에서 소유자의 정당한 권리 행사를 위한 처리는 합법적 논리에 따라 허용

- 드론을 이용해 토지 무단침입을 감시할 경우, 무단 침입자에게 동의를 받기는 현실적으로 불가능하고, 토지 소유자의 드론 개인정보 처리는 자신 소유상품 및 재산보호를 위한 정당한 권리 행사로 개인정보 처리를 위한 법적 근거를 확보한 것으로 인정

▶ DPC는 백서에서 아일랜드 리버릭시 당국과 의회의 드론 무단 사용 조사에 대한 결과를 사례로 제시하고, 공공 기관의 드론 활용에 대해 명확한 규정 준수를 요구

- DPC는 아일랜드 리버릭시가 드론 개인정보보호에 대한 법을 제정하지 않은 상태에서 2018년부터 폐기물 처리 감시 등에 드론을 사용했고, 우발적으로 찍힌 쓰레기 투하자 영상을 이용해 법 집행을 한 행위는 개인정보보호법 위반이라고 결론

- DPC는 리버릭시에 드론 촬영 위치와 운영 등에 대한 상세 정보를 웹사이트를 통해 개인정보 주체들에게 제공할 것과 11만 유로의 과징금을 부과

표2 _ 아일랜드 리버릭시의 드론 개인정보 침해 사례

- DPC는 2021년 아일랜드 리버릭시와 카운티 의회(Limerick City and County Council)의 드론을 이용한 법 집행 위법성 조사에서 시와 의회가 개인정보보호법과 관련 규정을 위반했다고 결론
- 리버릭시는 2018년 당시 폐기물 처리나 수질 오염 방지 등에 2대의 드론을 감시 용도로 사용했다고 인정했지만, 사람들의 사진 촬영에는 활용하지 않았다고 주장
- 하지만 DPC는 리버릭시가 폐기물 처리 과정에서 쓰레기를 버리는 사람이 우발적으로 찍힌 영상을 범죄 조사 목적으로 개인정보 처리했고, 이를 일반 대중에게 공개하지 않은 사실을 확인
- DPC는 리버릭시 행위는 드론에 의해 수집된 개인정보가 처리될 경우, 공개해야 한다는 2018년 개인정보보호법 제90조 위반이라고 결론
- 또 DPC는 리버릭시 의회가 2018년에 이미 범죄 탐지 등에 드론을 사용하고 있었지만, 드론 사용 관리를 위한 개인정보보호 정책이 없었다는 점을 확인하고, 이 역시 법 위반이라고 결론
- DPC는 리버릭시와 의회가 법 집행을 위해 사용되는 드론 사용에서 개인정보 주체가 요구하는 모든 정보를 제공하도록 한 규정과 상세한 드론 정책을 웹사이트 등을 통해 쉽게 접근할 수 있도록 해야 하는 의무를 위반했다고 결론
- 최종적으로 DPC는 리버릭시에 법적 근거 없이 CCTV를 이용한 모니터링과 드론 영상을 활용한 개인정보 처리 등에서 GDPR과 2018년 개인정보보호법을 위반했다고 결론짓고, 관련 내용 시정과 11만 유로 과징금을 부과

5. 시사점

▶ **(현재 규제 수준)** 미국 시민단체들은 BVLOS 드론이 기술 진보로 인해 개인정보 침해 가능성이 크게 높아졌으나, 현 규제로는 해결할 방안이 없다는 점을 우려

- EEF 등 시민단체들은 현 드론을 비롯한 공공장소의 항공 감시에 관한 법률이 모호하고, 드론의 광범위한 가용성에 비해 시민 개인정보를 충분히 보호할 수준에 도달하지 못했다고 평가

▶ **(상황에 맞는 효율성 채택)** 하지만 EEF 등은 동시에 항공 규제 당국 FAA가 BVLOS 드론의 개인정보 침해 해결을 위해 비행 제한지역 등을 설정하는 것은 비효율적 조치로 반드시 피해야 할 접근이라고 주장

- 장기적으로 드론의 개인정보 침해 문제는 사회와 시민이 드론의 비행 여부, 장소, 조건 등을 어느 선까지 허용하느냐하는 수용의 문제이기 때문에 획일적 기준 대신 상황에 맞는 절충이 적합하다는 주장

- 동시에 드론의 장점 및 안정성에 대해 시민이 느끼는 기대감 또는 우려는 예측할 수 없기 때문에 이를 획일적으로 반영한다는 것은 심각한 모순이라고 지적

▶ **(개인정보보호 도입 원칙)** 효과적인 드론 개인정보보호를 위해서는 ▲상세한 드론 정보 공개 및 쉬운 접근을 보장하는 투명성 확보 ▲개인정보 수집 최소화의 법제화 ▲다양한 이해관계자의 참여 등이 필요하다는 지적

- 미국과 EU 개인정보보호 시민단체는 투명성과 합리적인 커뮤니티 통제가 삶의 질에 대한 민주적 통제를 가능케 하는 최선의 방법이며, 개인정보보호 및 기타 문제를 구체적으로 해결하는 최선의 접근이라고 주장

▶ **(신기술과 개인정보보호)** 한편, 드론의 개인정보보호를 둘러싼 최근 논의는 향후 미래 사회의 개인정보보호에서 중요한 잣대가 될 것이라는 평가

- 현재 드론은 육안이나 소리로 식별이 어려울 만큼 높게 날 수 있고, 드론이 주변이 있다는 사실을 알았더라도 드론이 어떤 정보를 수집하는지를 알 수 있는 실질적 방법이 없음
- 드론 감시로부터 개인정보를 보호하는 것은 전적으로 드론 운영자에 달려 있는 상황
- 신기술의 부정적 영향은 취약점을 파고들어 확산하는 특징을 가져 드론의 개인정보 침해 우려를 방치할 경우, 개인정보 침해가 전 산업으로 확산될 것이라는 우려가 제기
- 드론 개인정보보호 대안인 투명성, 정보 접근성, 이해관계자의 참여 확대 등의 논의 체계 구축은 향후 새로운 기술로 인한 개인정보 위협에 활용할 수 있는 모델이라는 평가

Reference

1. DataGuidance, Ireland: DPC issues guidance on use of drones, 2022.6.27.
2. DPC, Guidance on the Use of Drones, 2022.5.
3. EFF, Letter of dissent to BVLOS UAS ARC Report, 2022.3.3.
4. EFF, Over-the-Horizon Drones Line Up But Privacy Is Not In Sight, 2022.8.29.
5. EFF, Privacy Considerations for BVLOS Drones: Privacy Considerations for FAA Aviation Rulemaking Committee on Beyond Visual Line of Sight Drone Flights, 2021.12.
6. FAA, Remote Identification for Drone Pilots, 2020.
7. FAA, Unmanned Aircfaft System Beyond Visual Line of sight Aviation Rulemaking committee, 2022.3.10.
8. Mirror, British teenager wins $250,000 DRONE-RACING prize at World Drone Prix in Dubai, 2016.3.14.
9. National Archives, Code of Federal Regulations, Title 14 Chapter I Subchapter F PART 107 - SMALL UNMANNED AIRCRAFT SYSTEMS
10. Wiley, FAA Committee Releases BVLOS Recommendations, 2022.3.14.

개인정보 국외이전 주요 정책 동향에 대한 OECD 분석과 시사점

[목 차]

1. OECD의 개인정보 국외이전 정책 분석 배경

▶ 오늘날 개인정보가 사물인터넷, 인공지능 등 최신 기술을 활용한 산업 혁신의 핵심 원천이 됨에 따라 국경을 넘는 개인정보 전송과 공유의 중요성이 강하게 부상

- 개인정보가 전 세계적 데이터 경제의 중요한 자원으로서 정당한 위치를 차지함에 따라 국내 및 국제적으로 개인정보 공유를 촉진하기 위해 신뢰를 구축하고 발전시키는 것이 중요

▶ 국경을 넘는 일상적인 대규모 개인정보 국외이전에 대한 정부, 기업, 개인의 우려가 증가하면서 주요국에서 법 집행이나 감사, 정부의 개인정보 주체 접근권 보장 등의 이유로 개인정보 국외이전 관련 정책 및 규제 역시 증가 추세

- 주요국 정부는 개인정보가 기밀이나 민감정보를 포함할 수 있어 개인정보보호 또는 보안 관점에서 개인정보 국외이전 관련 정책과 규제 강화

- 또한 개인정보가 디지털 산업 정책의 중요한 자원으로 작용하므로 디지털 집약적 산업에서 개인정보 관련 자국 역량을 개발하기 위해 개인정보 국외이전 관련 규제 적용

▶ 그러나 개인정보 국외이전을 관리하는 정책 및 규제가 다층적이고 엄격한 경우, 기업 등 경제주체가 국경을 넘어 개인정보를 공유하거나 공공 정책에서 개인정보를 이용할 때 추가 비용, 운영 복잡성 및 불확실성을 초래

- 개인정보와 관련한 국제 규제 환경변화에 따라, 최근 G20, G7[15] 등 국제 커뮤니티는 신뢰를 바탕으로 개인정보 국외이전을 촉진하기 위한 국제적인 협력과 대화, 절차 마련 등 정책적 노력을 활발히 추진

▶ 한편 최근 경제협력개발기구(OECD) 과학기술혁신국은 G7 디지털 및 기술 트랙(Digital and Technology Track)의 논의를 알리기 위해 개인정보 국외이전에 관한 전 세계 정책 및 전략에 관한 보고서[16] 발간(2022.10)

- 본 보고서는 OECD의 보고서 내용에 기반하여 '신뢰할 수 있는 개인정보 국외이전'(Data Free Flow with Trust, 이하 DFFT) 관련 ▲일방적 정책 및 규제 ▲정부 간 협약 ▲기술 및 조직적 조치에 관한 주요 정책과 법령을 소개하고, 정책적 시사점을 도출하고자 함

그림 _ 신뢰할 수 있는 개인정보 국외이전(DFFT)을 위한 주요 정책 및 프로세스

출처: OECD(2022.10)

15) G7: 정식명칭은 Group of Seven Summit. 주요 선진 7개국 정상회의를 뜻하며, 7개국은 미국, 영국, 프랑스, 독일, 일본, 이탈리아, 캐나다로 구성. 여기에 우리나라를 비롯해 중국, 인도 등 신흥경제국 13개국을 합쳐 G20이라 칭함

16) OECD, Cross-border Data Flow – Taking Stock of Key Policies and Initiatives, 2022.10

2. 일방적 정책 및 규제(Unilateral policies and regulations)

▶ 지난 수십 년 동안 국가들은 신뢰를 구축하기 위한 노력의 일환으로 개인정보 국외이전을 통제하기 위한 국가 단위의 일방적인 정책과 규제를 개발하고 구현했으며 이러한 정책과 규제는 다음 사항에서 공통된 요소를 공유

- 다른 공공 정책 목표를 보호하면서 개인정보 국외이전이 가능하도록 하는 공동의 목적 공유
- 정책 및 규제가 공동의 목적을 실현하기 위해 사용하거나 인식하는 조항, 메커니즘 및 도구를 점진적으로 더욱 많이 공유

▶ 이중 국가의 일방적인 정책 및 규제에 따르는 조항 또는 메커니즘은 다음 두 가지 주요 범주로 구분 가능

- **(오픈 보호조치, Open Safeguards)** 요구사항을 충족해야 하는 방법에 관한 명시적 규정이 없이 공공 정책 목표의 지속적 보장을 위해 개인정보를 전송하는 국가의 기관에 전적으로 의존

  - 예를 들어 이 경우 사후 책임 원칙에 따라 개인정보를 국외에 전송하는 국내 기업은 개인정보를 수신하는 국외 기업이 현지 법률의 요구사항에 부합하는 방식으로 개인정보를 처리하는지 확인하고, 개인정보를 전송하는 국내 기업의 일반적인 요구사항을 계약 형태로 보호하고, 개인정보 국외이전 이후에 보호 수준을 충분히 평가해야 함

- **(사전 승인 보호조치, Pre-authorised safeguards)** 신뢰할 수 있는 개인정보 국외이전을 보장하기 위해 정부 당국이 적극적으로 사전 승인 형태를 취함

  - 예를 들어 이 경우에는 ▲정부 당국이 개인정보 수신 국가의 화이트리스트 작성 ▲공공 부문이 사전 승인한 특정 조항(표준이나 계약 모델의 조항)을 개인정보 국외이전 계약에 통합 ▲구속력 있는 기업 규칙으로 사전 승인 ▲직접(국가의 공식적 인증제도) 또는 간접(민간 인증을 인정) 방식으로 모니터링 수행 등이 해당

▶ 최근 몇 년 동안 점점 더 많은 국가에서 '사전 승인 보호조치 메커니즘'에 기반한 개인정보 국외이전에 관한 계약 모델을 발표

- 정부 당국은 개인정보 감독기구와 협력하여 국외이전 개인정보를 공유하려는 주체(기업/기관 등) 간 권장 또는 의무사항으로 계약 조항을 규정할 수 있으며, 이러한 조항들이 계약에 통합된 경우 합법적인 개인정보 전송으로 간주

- 최근 EU, 뉴질랜드, 영국, 아르헨티나 등이 사전 승인 보호조치에 기반한 계약 조항*을 개발

* EU의 GDPR과 연계되어 최근 개정된 표준계약조항(Standard Contractual Clauses, SCCs), 뉴질랜드의 모델 계약 조항, 영국의 국제 개인정보 전송 계약(International Data Transfer Agreement), 아르헨티나의 개인정보보호 계약 조항 등이 있음

- 2021년 동남아시아국가연합(ASEAN)도 개인정보 국외이전을 위한 일련의 계약 조항 발표

3. 정부 간 프로세스(Inter-governmental processes)

(1) G7 및 G20의 주요 관련 심의

▶ 협력을 증진하고, 신뢰할 수 있는 개인정보 국외이전(DFFT)을 가능하도록 정부 간 포럼에서 다음과 같은 프로세스 진행 중

- G7 및 G20의 개인정보 국외이전에 관한 심의
- 다자간 기구에서 대화를 촉진하는 표준 설정 노력, 연구 및 분석 이니셔티브 추진
- 지역 파트너 간 표준 설정 또는 구속력 있는 계약 개발
- 다양한 특정 유형의 무역 협정 체결

▶ **(G7 및 G20의 심의)** 지난 몇 년 동안 G7 및 G20의 심의에서는 DFFT 촉진의 중요성을 점점 더 강조

표1 _ G7 및 G20의 주요 심의 내용

연도	주체	주요 내용
2019	G20	• G20 무역 및 디지털 경제 장관 성명(G20 Ministerial Statement on Trade and the Digital Economy) (6월) - 개인정보 국외이전 관련 개인정보 보호, 지식재산권 및 보안 관련 이슈 인식하고, 개인정보를 포함하지 않는 데이터 전송에 관한 협력을 촉진하여 소비자와 기업의 신뢰를 강화하고, 서로 다른 체계의 상호운용성을 장려하기 위해 협력
2020	G20	• G20 리야드 지도자 선언(Riyadh Leaders' Declaration) (11월) - 개인정보가 포함되지 않은 데이터 전송을 촉진하고 소비자와 기업의 신뢰를 강화하기 위한 합의를 재확인
2021	G7	• 신뢰할 수 있는 개인정보 국외이전에 대한 협력을 위한 G7 로드맵(G7 Roadmap for Cooperation on Data Free Flow with Trust) (4월) - 개인정보보호, 지식재산권, 보안과 관련된 문제를 계속 해결하면서 우리 경제와 사회에서 개인정보 활용의 중요성 강조

연도	주체	주요 내용
		- 개인정보가 포함되지 않은 데이터 전송의 이점을 실현하는 작업을 지원하기 위해 민주적이며 개방적이며 공유된 가치 활용 • G7 통상 장관은 디지털 무역 원칙(Digital Trade Principle) 개발(10월) - 개인과 기업의 신뢰를 바탕으로 개인정보 국외이전이 가능해야 함
	G20	• G20 로마 지도자 선언(G20 Rome Leaders' Declaration) (11월) - 신뢰에 기반하고, 개인정보를 포함하지 않은 데이터 전송의 중요성 인정 - 특히 미래의 상호운용성을 촉진하기 위해 기존 규제 접근 방식과 개인정보를 신뢰할 수 있는 방식으로 전송할 수 있도록 도구 간의 공통성, 보완성 및 수렴 요소를 식별하기 위해 노력하고 공동의 이해를 유지하기로 합의
2022	G7	• G7 디지털 장관 선언(G20 Ministerial Statement) (5월) - 혁신, 번영, 민주적 가치를 지지 • 신뢰할 수 있는 개인정보 국외이전(DFFT) 촉진을 위한 G7 실행계획(G7 Action Plan for Promoting Data Free Flow with Trust) (5월) - DFFT에 대한 증거 기반 강화, 미래 상호운용성을 촉진하기 위한 공통점 구축, 지속적인 규제 협력 및 디지털 거래의 맥락에서 DFFT 촉진

출처: OECD(2022.10)

▶ 2022년 G7 디지털 및 기술장관회의(의장국: 독일)는 혁신, 번영 및 민주적 가치의 버팀목으로서 DFFT의 역할을 선언하고 개인정보 국외이전 촉진을 위한 G7 실행계획 채택

- 규제 협력, 디지털 통상에서의 DFFT 촉진
- G7 디지털 장관은 G7 공동의 열망과 이번 G7의 선언을 기반으로 개인정보보호 당국의 원탁회의를 통한 DFFT 규제협력 촉진 등을 지속하려는 2023년 의장국인 일본의 목표를 환영
- G7 국가들은 신뢰를 통한 DFFT 촉진을 약속하며, 이를 위해 G7 디지털 장관은 DFFT에 대한 영국의 2021 G7 협력 로드맵에서 설정한 4가지 전략적 기둥(Pillars), 즉 (1) 규제 협력, (2) 개인정보 현지화, (3) 민간 부문이 보유한 개인정보에 대한 정부의 접근, (4) 우선순위가 높은 부문의 개인정보 공유에 관한 문제를 해결하기 위해 협력 지속

  - G7 국가는 개인정보 공유 접근 방식에 대한 정략적 기둥 하에서 국제 개인정보 공간에 대한 지식 공유에 대한 새로운 초점에 주목

- G7 국가들은 공동으로 신뢰를 통한 개인정보 국외이전 촉진을 위해 전념하여 실행할 과제와 주요 내용을 다음과 같이 제시

표2 _ G7 실행계획의 실행과제 및 주요 내용

실행과제	주요 내용
1. DFFT 지원을 위한 증거 기반 강화	• 개인정보 국외이전으로 발생하는 기회와 과제를 이해하기 위해 노력 • 개인정보보호, 보안 및 지식재산권 보호를 포함하여 DFFT를 가능하게 하는 기존 규제 접근 방식 및 도구에 대한 이해 심화 • 중소기업에 대한 영향을 포함하여 개인정보 현지화 조치 및 잠재적 영향을 이해하고 현지화에 대한 대안을 고려
2. 미래의 상호운용성을 촉진하기 위한 공통기반 구축	• 미래의 상호운용성을 촉진하기 위해 기존 규제 접근 방식과 신뢰할 수 있는 개인정보 전송이 가능하도록 도구 간 공통, 보완, 수렴하는 요소 기반 구축 • 표준 계약 조항 등 일반적인 절차, 신뢰 강화 기술의 잠재력에 대한 추가적 분석 • 신뢰할 수 있는 정부의 민간이 보유한 개인정보 접근 등 공통 관행을 식별하기 위해 OECD 작업을 계속 지원
3. 지속적인 규제 협력	• G7 정책관계자, 개인정보 감독기구, 기타 개인정보 관련 권한 있는 당국 간의 대화 등 DFFT에 대한 규제 협력을 촉진 • 개인정보보호 강화기술(PET), 개인정보 중개자, 웹 추적, 국가 간 샌드박스, 개인정보보호 체계의 상호운용성 촉진, 신뢰할 수 있는 정부의 개인정보 접근에 대한 OECD 추진활동, 글로벌 개인정보보호총회(2021.10)의 개인정보에 대한 정부 접근 결의와 관련된 규제적인 접근법 논의 • UN PET Lab과 같은 프로그램에 적극적인 참여 • 개인정보보호 및 관련 법률 및 규제 시행에 대한 개인정보보호 및 개인정보보호 당국 간 협력을 포함하여 DFFT에 대한 규제 협력을 촉진하기 위한 노력을 지원
4. 디지털 통상의 맥락에서 DFFT 촉진	• 2021년 G7 통상 트랙(G7 Trade Track in 2021)에서 개발한 디지털 통상 원칙(Digital Trade Principles) 기반으로 DFFT 촉진 • 전자상거래에 관한 공동 성명 이니셔티브(Joint Statement Initiative on E-Commerce)의 결과에 대해 WTO 논의를 지원
5. 국제 개인정보 공간의 전망에 대한 지식 공유	• "국제 개인정보 공간"에 대한 지식교류를 촉진하고 정책환경 활성화 • 개인정보 공간은 학계, 산업체 및 공공 부문의 혁신을 지원하기 위해 국내 또는 국제적으로 조직 및 부문 간에 신뢰할 수 있고 자발적인 개인정보 공유에 대한 새로운 접근 방식으로 간주

출처: G7 Germany(2022)[17]

(2) 다자간 접근(Multilateral approaches)

▶ OECD는 2021년 10월 다양한 국가의 상황과 규제체계의 차이점을 고려하고, 국제적인 논의 등을 거쳐 "개인정보 접근 및 공유 강화(Enhancing Access to and Sharing of Data, EASD)에 관한 권고사항"[18] 마련

17) G7, G7 Digital Ministers' Track - Annex 1 G7 Action Plan for Promoting Data Free Flow with Trust, 2022 https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile

- 정부가 산업부문, 국가, 조직, 커뮤니티 전반에 걸쳐 그리고 정부 내에서 개인정보의 잠재적 이점을 실현하기 위해 일관된 개인정보 거버넌스 정책 및 프레임워크 개발 지원

  - 개인정보 생태계 전반에 걸쳐 신뢰를 강화하고, 개인정보 투자를 촉진하고, 개인정보 접근 및 공유를 장려하고, 국가 및 산업 전반에 걸쳐 효과적이고 책임감 있는 개인정보 접근, 공유 및 사용을 촉진

- 정부가 개인과 조직 권리를 보호하고 기타 정당한 이익과 목표를 고려하면서 개인정보 접근 및 공유 협정을 강화하는 이점을 극대화하는 방법에 관한 일반 원칙과 정책 지침 설정

- OECD는 '개인정보 접근 및 공유 강화에 관한 권고사항'에서 3개 영역(Section)과 7개 주제(Theme)를 제시

표3 _ G7 실행계획의 실행과제 및 권고사항 내용

3대 영역	7대 권고사항
개인정보 생태계 전반에 걸친 신뢰 강화	• 개인정보 생태계의 신뢰성을 높이기 위한 광범위한 노력과 함께 모든 관련 이해관계자에게 권한을 부여하고 적극적으로 참여하도록 독려 • 개인정보 접근 및 공유에 대한 전략적 범정부적 접근방식 채택 • 개인과 조직의 권리를 보호하고 개인정보 거버넌스에 대한 책임 문화를 촉진하고 활성화하기 위한 광범위한 노력과 함께 정당한 이익과 목표를 고려하면서 개인정보 접근 및 공유의 이점 극대화
개인정보 투자 촉진 및 개인정보 접근 및 공유 장려	• 일관된 인센티브 메커니즘을 제공하고 개인정보 접근 및 공유에 대한 지속 가능한 사업 모델과 시장을 창출 및 채택할 수 있는 환경 조성
사회 전반에 걸쳐 효과적이고 책임감 있는 개인정보 접근, 공유 및 사용 촉진	• 국경을 초월한 개인정보 접근 및 신뢰 공유를 위한 환경을 개선 • 공공 및 민간 부문 조직 전반에 걸쳐 개인정보의 검색 가능성, 접근성, 상호 운용성 및 재사용 가능성 촉진 • 개인정보 가치주기(Value Cycle)에 따라 개인정보를 책임감 있게 효과적으로 사용할 수 있도록 모든 이해관계자의 역량 강화

출처: OECD(2021.10)

18) OECD, Recommendation on Enhancing Access to and Sharing of Data, 2021.10. https://www.ospi.es/export/sites/ospi/documents/documentos/OECD-Recomendacion_Acceso_y_Mejora_Comparticion_Datos_202110.pdf

▶ 2022년 1월 UN의 공식 통계를 위한 빅데이터 및 데이터 사이언스 전문가위원회(UN Committee of Experts on Big Data and Data Science for Official Statistics)는 개인정보보호 강화기술(PET)을 사용하여 국제적인 개인정보 공유를 안전하게 만드는 프로그램을 시범 운영하는 특정 목표를 가진 UN PET Lab 개시[19)]

- UN PET Lab은 통계 기관을 모으고 PET 기술을 제공하는 기술 제공업체와 협력하여 국외이전 개인정보를 전송하는 솔루션을 테스트하는 파일롯 프로젝트 개시

- UN PET Lab의 파일럿 프로젝트에는 ▲미국 인구조사국(US Census Bureau) ▲네덜란드 통계청(Statistics Netherlands) ▲이탈리아 국립통계연구소(Italian National Institute of Statistics) ▲영국 통계청(Office for National Statistics)이 참여

(3) 지역협정(Regional arrangements)

▶ **(ASEAN)** 2021년 1월 첫 번째 아세안 디지털장관회의(ADGMIN)는 개인정보 국외이전에 대한 모델계약조항(Model Contractual Clauses for Cross Border Data Flows, MCCs) 승인

- MCCs는 국경을 넘어 서로 개인정보를 전송하는 기업 간 구속력 있는 법적 계약에 포함될 수 있는 계약 조건 기술

- 중소기업의 경우 협상 및 규정 준수 비용과 시간을 줄이는 데 도움이 되는 동시에 개인정보 국외이전에서 개인정보보호를 강화

▶ **(EU)** 2022년 6월 23일 EU 데이터거버넌스법(Data Governance Act, DGA) 발효

- DGA는 회원국 간 개인정보 거버넌스를 조화시키고, EU 내 모든 유형의 개인정보 국외이전을 보장하기 위해 전자 개인정보 처리를 규제

- 특정 범주의 공공 부문 개인정보의 재사용을 촉진하는 메커니즘을 설정하고 개인정보 중개 서비스(Data intermediation service) 및 개인정보 이타주의(data altruism) 등 촉진

  - 동 법은 개인정보를 공유하는 개인이나 기업의 보안 강화를 목표로 개인정보 중개 서비스에 대한 조건을 규정하며, 개인정보 중개 서비스 제공자(data intermediaries)는 동 법에 따라 그 역할이 거래 중개에 국한되는 중립적인 제공자로서 행동해야 함

  - 개인과 기업이 일반적인 이익을 위해 동의를 기반으로 개인정보를 쉽게 공유할 수 있도록 개인정보 이타주의 도입

- 특히, 非개인정보(non-personal data)에 대한 적절성 결정 및 표준 계약 조항과 같은 메커니즘 등 개인정보 국외이전에 대한 규칙 규정

19) UN, UN PET Lab Open House, 2022.11.08.(확인)
https://unstats.un.org/bigdata/events/2022/un-pet-lab/april-open-house/

(4) 특혜무역협정(Preferential trade agreements)

▶ 2021년 5월 1일 EU-영국 무역 및 협력 협정(TCA, Trade and Cooperation Agreement)[20] 발효

- 개인정보 국외이전을 포함한 개인정보보호에 대한 조치는 이전된 개인정보보호를 위한 일반적인 조건 하에서 전송을 가능하게 하는 수단(Instruments)을 포함해야 한다는 조항을 도입

▶ 2022년 6월 영국과 싱가포르의 경우 디지털 경제 협정(UKSDEA) 서명 등 국가들은 인공지능에서 디지털 결제에 이르기까지 다양한 문제를 다루는 보다 광범위한 디지털 경제 협정 협상을 시작

- 새로운 유형의 거래 계약에는 특정 예외에 따라 개인정보보호 체계 유지 및 개인정보 국외이전 허용에 대한 구속력 있는 조항이 포함되는 경우가 다수

4. 기술·관리적 조치(Technological and organisational measures)

▶ 수많은 다양한 주체가 방대한 양의 개인정보를 생성·보유하고 있지만, 신뢰 이슈, 개인정보 공유를 방해하는 요인, 국경이전 개인정보에 대한 검색 및 접근 관련 운영 문제 등으로 정부기관, 기업, 개인들이 최대의 혜택을 얻지 못하고 있음

▶ 이러한 문제점을 인식하여 정부, 산업, 국가 간의 장벽을 허물고 문제점을 해결하기 위한 기술적, 관리적 조치를 마련하기 시작

- 개인정보 중개 서비스 제공자의 경우 개인정보 공유 행위자 간 관계에서 기술적, 관리적 측면에서 서비스를 제공하며, 개인정보보호 강화기술(PET) 등을 이용하여 민감정보를 안전한 방식으로 이용할 수 있도록 지원

▶ 2022년 2월 EU 집행위원회(EC)가 제안한 유럽데이터법안(European Data Act)은 개인정보에 대한 공정한 접근과 이용을 촉진하며, 공통 유럽 개인정보 공간* 관련 다음의 기능을 포함하도록 함

* Data Space: 디지털 경제에서 협력을 가능하게 하고 진입 장벽을 낮추며 혁신을 촉진하기 위한 목적으로 개방적이고 투명한 표준을 기반으로 개인정보를 공유하는 시스템

20) Treaty Section, Foreign, Commonwealth and Development Office,, Trade and Cooperation Agreement, 2021 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/982648/TS_8.2021_UK_EU_EAEC_Trade_and_Cooperation_Agreement.pdf

- 개인정보 접근, 공유, 처리 및 사용하기 위한 안전하고 개인정보를 보호하는 인프라
- 공정하고 투명하며 비례하고 非차별적인 방식으로 개인정보에 접근하고 사용하기 위한 명확하고 실용적인 구조와 명확하고 신뢰할 수 있는 개인정보 거버넌스 메커니즘
- 유럽의 규칙과 가치, 특히 개인정보보호, 소비자 보호 법률 및 경쟁법을 철저히 준수
- 개인정보 소유자는 개인정보 공간에서 자신이 통제하는 특정 개인 또는 非개인정보에 대한 접근 권한을 부여하거나 공유 가능
- 개인정보를 무료로 재사용 가능
- 조직/개인 인원의 제한 없는 참여

5. 결론 및 시사점

▶ 개인정보 국외이전은 디지털 기술의 잠재력을 실현하고 혁신적인 비즈니스 모델을 창출하며, 전 세계에서 개인정보를 이동 및 활용하는 서비스의 기존 모델을 향상하는 데 매우 중요

- 기업, 시민, 사회를 위한 개인정보 국외이전에 대한 높은 수준의 신뢰성 유지와 개인정보보호 표준 유지는 국제경제를 위한 디지털 혁신의 이점을 실현하는 데 중요

▶ 최근 국제 개인정보보호 관련 커뮤니티를 중심으로 신뢰할 수 있는 개인정보 국외이전을 지원하기 위한 공통 표준, 메커니즘 및 규정 개발 등의 활동이 활발하게 진행 중

- 주요국 정부는 신뢰할 수 있는 방식으로 국가 간 개인정보 공유를 촉진하기 위해 협력을 지속적으로 추진

▶ 향후 사물인터넷이나 인공지능 등 최신 기술을 이용한 서비스 제공에 국외이전 개인정보 활용이 증가할 것으로 예상됨에 따라, 신뢰할 수 있는 정부 당국이 구체적인 장벽을 찾아 해결하는 정책적, 기술적 노력 강화 필요

- 개인정보가 국가 경제 및 사회 발전에 기여하도록 개인정보의 잠재력을 최대한 활용하는 미래 정책 및 규제 접근 방식을 지원
- 신뢰할 수 있는 개인정보 국외이전을 촉진하기 위한 실용적인 솔루션을 제공하는 정책 환경의 설계를 위해 주요국 등의 관련 정책 당국과 국제 협력 필요

Reference

1. G7, G7 Digital Ministers' Track - Annex 1 G7 Action Plan for Promoting Data Free Flow with Trust, 2022
2. OECD, Cross-border Data Flow – Taking Stock of Key Policies and Initiatives, 2022.10
3. OECD, Recommendation on Enhancing Access to and Sharing of Datahttps: 2021.10.
4. Treaty Section, Foreign, Commonwealth and Development Office, Trade and Cooperation Agreement, 2021

〈2022년 개인정보보호 월간 동향 보고서 발간 목록〉

번호	호수	제 목
1	1월 01	EDPB, 개인정보 침해 통지에 관한 가이드라인 발행
2	1월 02	EDPB, EU 집행위의 데이터 관련 법안 관련 성명 발표
3	1월 03	CJEU 법무관, 정보 주체 위임 없는 소비자단체의 대리 제소 관련 의견서 발표
4	2월 01	해외 주요국 아동·청소년 개인정보보호 법제도 정비 동향
5	2월 02	EU 데이터 관련 법안 법제화 추진 현황
6	2월 03	2022년 초 맞춤형 광고 시장에 발생한 주요 변수
7	3월 01	2022년 주요 개인정보보호 실태 서베이 보고서 분석
8	3월 02	유럽과 미국의 안면인식 관련 주요 동향
9	3월 03	시행 4주년 앞둔 GDPR, 최근 집행 이슈와 그간의 성과
10	4월 01	클라우드 서비스 관련 개인정보보호 이슈 및 해외 규제 동향
11	4월 02	개인정보 보호 약화 논란에 직면한 EU 법안들
12	4월 03	블록체인 기반 스마트계약 개인정보보호 이슈 및 정책동향
13	5월 01	중국 개인정보 국외처리를 위한 인증의 주요 내용과 시사점
14	5월 02	미국 연방 개인정보보호법안(ADPPA) 주요 내용과 시사점
15	5월 03	미국과 EU, 다크패턴에 대한 감독 강화 추진
16	6월 01	EDPB의 GDPR 위반 과징금 산정에 관한 가이드라인(초안) 주요 내용 분석
17	6월 02	키스트로크 로깅 기반 원격근무자 감시 관련 미국 개인정보보호 법제 추진 동향
18	6월 03	영국 개인정보 개혁 정책 방향 담은 '정부 대응 문서' 주요 내용 분석
19	7월 01	GDPR 체계하에서 메타버스 관련 개인정보 이슈 분석
20	7월 02	영국 ICO의 발전 전략을 담은 'ICO25' 분석 및 시사점
21	7월 03	해외 주요 개인정보 감독기구 연례보고서 주요 내용 및 활동 성과(1)
22	8월 01	자율주행차 관련 영국과 캐나다의 개인정보보호 정책·법제 사례 분석
23	8월 02	헬스케어 분야 개인정보보호 강령 사례 분석
24	8월 03	Clearview AI 관련 유럽 개인정보 감독기구 행정처분 주요 내용
25	9월 01	영국 정보주체 접근요청(DSAR) 현황과 시사점

26	9월 02	드론 이용 확산에 따른 개인정보보호 이슈 분석
27	9월 03	개인정보 국외이전 주요 정책 동향에 대한 OECD 분석과 시사점

2022
개인정보보호 월간동향분석 9월호

발 행 2022년 12월 7일

발행처 한국인터넷진흥원
전라남도 나주시 진흥길 9
Tel: 061-820-1899