데이터 보안 및 비식별화 정책

Q1. 통신사에서 수집하는 개인정보의 주요 범주는 무엇인가요?
A1. 주요 수집 항목은 다음과 같습니다:
- 가입자 정보 (이름, 생년월일, 연락처, 주소 등)
- 요금 및 결제 정보
- 통신 이력 (통화, 메시지, 데이터 사용 내역)
- 위치 정보 (Cell ID, GPS 등)
- 단말 정보 (IMEI, OS 등)
이들은 서비스 제공과 과금, 품질 개선, 고객 대응에 사용됩니다.

Q2. 개인정보 처리의 주요 원칙은 무엇인가요?
A2. 다음의 원칙이 적용됩니다:
- 최소 수집 원칙
- 목적 명시 및 제한 원칙
- 정보 주체 권리 보장
- 보안성 확보 의무
- 보유 기간 제한
이는 [개인정보 보호법] 및 [통신비밀보호법]에 기반합니다.

Q3. 데이터 비식별화란 무엇이며 왜 필요한가요?
A3. 데이터 비식별화란 특정 개인을 식별할 수 없도록 데이터에서 식별자를 제거하거나 대체하는 과정입니다.
주요 목적은: 개인정보 보호, 데이터 활용 촉진 (예: 통계, AI 모델 학습), 법적 규제 준수입니다.

Q4. 데이터 비식별화를 위한 주요 기술은 어떤 것이 있나요?
A4. 대표적인 기법은 다음과 같습니다: 총계처리 (Aggregation), 마스킹 (Masking), 가명처리 (Pseudonymization), 랜덤 노이즈 삽입 (Differential Privacy), 일반화 (Generalization)
이들은 사용 목적과 민감도에 따라 적절히 조합됩니다.

Q5. 데이터 마스킹(Masking)은 어떻게 구현되나요?
A5. 예를 들어, 주민등록번호 900101-1234567은 900101-1******처럼 일부 정보를 별표(*)로 대체합니다.
이는 저장·처리·출력 시 노출을 최소화하고, 실시간 응답 시스템에도 적용됩니다.

Q6. 위치 정보는 어떻게 비식별화되나요?
A6. 위치 정보는 다음 방식으로 처리됩니다:
- Cell ID 단위로 일반화
- 시/군/구 등 행정단위로 변환
- 랜덤 Offset 추가
이 외에도 일정 수준 이하로 샘플링하거나, 시간 단위 집계를 적용합니다.

Q7. 비식별화된 데이터도 개인정보로 간주되나요?
A7. 원칙적으로 식별이 불가능한 경우 비식별 정보로 분류되어 개인정보 보호법 적용 대상이 아닙니다.
하지만 재식별 가능성이 존재하거나, 제3자 결합 시 식별될 여지가 있으면 여전히 보호 대상입니다.

Q8. 통신사의 데이터 보관 기간은 어떻게 설정되나요?
A8. 법령 및 내부 정책에 따라 다릅니다:
- 요금 관련 정보: 5년
- 통화/메시지 내역: 12개월
- 위치 정보: 최대 6개월
- 단말 접속 로그: 3개월 이상
보유 기간 경과 시 암호화 후 폐기 또는 완전 삭제됩니다.

Q9. 통신사가 외부 기관에 데이터를 제공할 수 있는 조건은?
A9. 다음과 같은 경우에만 제한적으로 제공됩니다:
- 이용자의 사전 동의
- 수사기관의 적법한 요청
- 통계청, 연구기관 등 공익 목적의 법적 근거 보유 기관
이 경우에도 비식별화 또는 최소 단위 제공이 원칙입니다.

Q10. 외부 데이터 제공 시 검토 및 승인 절차는 어떻게 되나요?
A10. 1. 요청 목적 및 법적 근거 확인
2. 내부 개인정보보호위원회 또는 법무 검토
3. 비식별화 수준 검토 및 보완 조치
4. 최종 책임자 승인 후 제공
이후 제공 이력은 로그로 관리되고 정기적으로 감사됩니다.

Q11. 통신사 내 개인정보 접근 통제는 어떻게 하나요?
A11.
- 직무별 접근 권한 최소화 (RBAC)
- 이중 인증(MFA), 접근 로그 기록
- 시간대 제한, IP 화이트리스트 적용
- 개인정보 처리 이력 자동 감사
이를 통해 내부자 오남용을 방지합니다.

Q12. 로그 데이터가 개인을 식별할 수 없도록 하는 방법은?
A12.
- 로그에 포함된 IP, UUID, 전화번호 등은 해시(SHA256)로 변환
- IMEI, IMSI는 암호화 또는 마스킹
- 세션 ID는 주기적 갱신 및 단방향 처리
이렇게 처리해도 통계나 품질 분석에는 문제가 없도록 설계합니다.

Q13. 비식별 처리 후에도 재식별 가능성이 높다면 어떻게 하나요?
A13.
- 결합 정보 제거 또는 무작위 처리 수준 강화
- 추가적인 익명화 기법 적용
- 정보 결합을 차단하기 위한 기술적 제한 (예: 파편화 저장)
이외에도 제3자 독립 검증 후 데이터 활용 여부를 결정합니다.

Q14. 내부 데이터 분석 부서에서 준수해야 할 규정은?
A14. 분석 목적과 범위 사전 등록 (데이터 활용 신청서 작성), 개인 식별 정보 접근 금지, 출력 데이터 사전 검토 (개인 정보 포함 여부), 분석 결과 저장소 별도 격리, 정기적 보안 교육 이수
모든 작업은 로그로 기록되어 감사 대상으로 포함됩니다.

Q15. 통신사의 데이터 보호 체계는 어떤 인증을 통해 검증되나요?
A15. 대표적인 보안 인증은 다음과 같습니다:
- ISMS-P (정보보호 및 개인정보보호 관리체계 인증)
- ISO/IEC 27001 (정보보호 국제표준)
- ISO/IEC 27701 (개인정보보호 국제표준)
이외에도 방송통신위원회 및 개인정보보호위원회의 연례 점검을 통과해야 합니다.