

구속력 있는 회사 규칙

- A. 서론
- B. 적용
- C. 범위
- D. 정책
- E. 참고자료
- F. 검토

발행일: 2017년 5월 15일
최근 검토일: 2020년 4월 3일
최근 개정일: 2020년 4월 3일

A. 서론

RTX는 자사의 이사, 임원, 직원 계약자, 고객, 공급자 및 벤더 등 개인 정보 처리 대상인 사람들의 정당한 프라이버시 권리를 존중한다.

RTX는 개인에 대해 처리하는 개인 정보에 대해 구속력 있는 회사 규칙("BCR")을 채택하였다. **United Technologies EU("RTX EU")**¹가 주도적 계열사로서 RTX 본사(미국 본사)와 협조하여 BCR 위반을 시정할 책임을 지고 있다.

별첨 A에서는 BCR에서 사용되는 용어와 약어의 정의를 설명한다.

RTX는 인사 정보(직원 및 도급 근로자), 비즈니스 고객, 공급사, 벤더, 영업 담당자 및 기타 비즈니스 파트너의 비즈니스 연락처 정보, RTX 제품 소비자들로부터 얻은 정보 및 이름, 주소 및 신용 카드 데이터와 같은 일반적으로 제한된 정보, 방문객 및 직원이 아닌 영업 담당자 및 유통업체에 관한 정보, 그리고 해당 제품과 서비스 사용자들의 RTX 제품 사용에 관하여 수집된 정보 전송한다. 개인 정보는 제공되는 제품과 서비스 및 특정 서비스나 프로젝트에 필요한 지원에 따라 RTX 내부에서 전송된다. 대부분의 개인 정보는 미국에 있는 RTX 본사로 전송된다.

B. 적용

1. BCR은 RTX 본사 및 그룹간 계약을 체결한 사업체들이 반드시 준수해야 한다. 해당 업체들은 자사의 직원들이 개인의 개인 정보를 처리할 때 BCR을 준수하도록 보장해야 한다. RTX는 BCR 준수를 위해 전사에 걸쳐 명확하고 일관된 통제 방안을 수립한다.
2. RTX는 최소한 전세계에서 당사에 적용되는 개인 정보 보호 관련 모든 법률과 규정을 준수해야 한다. 보다 높은 수준의 데이터 보호를 규정하여 RTX에 적용되는 현지 법률, 규정 및 기타 제한 사항은 BCR보다 우선적으로 적용한다. 해당 법률이 BCR과 상충하여 RTX의 본사 또는 한 개 이상의 사업체가 BCR에 근거한 의무를 이행하는 것이 방해로 받고 그에 명시된 보장 내용에 실질적 영향을 줄 경우, 해당 업체는 신속히 'RTX 최고 개인정보 보호 책임자'(RTX CPO)에게 통지해야 한다. 다만 법 집행 당국이나 법률에서 그러한 정보 제공을 금지하는 경우에는 예외로 한다. RTX CPO는 개인정보 자문 위원회와 해당 업체 및 사업부와 협조하여 적절한 행동 방침을 결정해야 하고, 확실하지 않을 경우 해당 데이터 보호 당국에 문의해야 한다.

¹ United Technologies EU, Avenue des Arts 58, 1000 Brussels.

3. 또한 BCR은 다른 RTX 업체를 대신하여 개인 정보를 처리하는 사업체와 본사에도 적용된다. 처리 업체는 해당 BCR의 별첨 B에 명시된 내부 처리 조항의 적용을 받는다.
4. BCR과 회사 정책 매뉴얼 섹션 24 사이에 상충되는 내용이 있을 경우, 유럽 경제 지역이나 스위스에서 직접 또는 간접적으로 들어오는 개인 정보에 대해서는 본 BCR을 우선 적용한다.

C. 범위

본 BCR은 RTX가 장소 불문하고 개인의 개인 정보를 처리하는 경우에 적용된다. 다만 (i) 민감한 개인 정보에 대해 명확한 동의를 받아야 하는 요건 (ii) 개인과 보증인의 이행 권리에 관하여 섹션 D.6의 1~6절에 포함된 조항 (iii) BCR과 회사 매뉴얼 섹션 24 간의 불일치에 관한 섹션 B.4 (iv) D.1(d)의 요건 및 (v) 법집행 당국 및 규제 당국과의 데이터 공유에 관한 섹션 D.1(f) 부분은 유럽 경제 지역, 영국 또는 스위스에서 직접 또는 간접적으로 들어오는 개인 정보에만 적용된다.

D. 정책

1. **개인정보 원칙:** RTX는 모든 활동에서 다음 사항을 준수해야 한다.

- a) *개인 정보를 공정하고 합법적으로 처리한다.*

개인 정보는 (1) 동의를 바탕으로 (2) 출처 국가의 법률이 허용하는 경우 또는 그 법률적 요구에 따라 (3) 합법적 목적(예: 인사 관리, 고객 및 공급사와 비즈니스 상호작용, 물리적 위협과 위협에 대응)을 위해 식별된 목적으로 처리해야 한다.

개인의 민감한 개인 정보는 (1) 데이터 출처 국가의 법률이 요구할 경우 (2) 법률이 허용할 경우 해당 개인의 명시적 동의를 받아 또는 (3) 개인의 귀중한 권리 보호를 위해 또는 본사나 사업체가 법적 클레임 규명, 행사 또는 방어를 위해 필요할 때에만 처리해야 한다.

개인 정보는 양립할 수 없는 목적으로 처리해서는 안 된다. 다만 직전 절에 명시된 조건 중 하나에 따라 예를 들어 새로운 동의를 받아서 처리하는 경우는 허용된다.

- b) *해당되는 개인 정보만 처리한다.*

RTX는 정보 처리의 목적과 관련하여 개인 정보의 처리가 적절하고 타당하고 과도하지 않도록 하기 위해 노력해야 한다. 또한 RTX는 수집 목적에 필요한

기간보다 길게 개인 정보를 유지해서는 안 된다. 다만 새로운 목적에 사용할 때 동의를 받은 경우 또는 해당 법률, 규정, 소송 절차, 행정 절차, 중재 절차 또는 감사 요건에 의해 달리 요구되는 경우는 그에 따른다. RTX는 보유 중인 개인 정보가 정확하고 최신 상태를 유지하도록 노력을 한다.

c) *사업체가 처리하는 개인 정보의 해당 개인에게 적절한 통지를 한다.*

개인이 이 정보를 이미 알고 있지 않을 경우, 본사 및/또는 해당 사업부는 개인 정보 수집 시에 개인에게 다음 사항을 통지해야 한다 - 수집 대상 개인 정보, 수집되는 개인 정보를 책임지는 RTX 업체의 신분 및 연락처 상세정보, 해당 정보 보호 책임자의 연락처 상세정보, 개인 정보 수집 목적, 통제자의 처리 법적 근거 및 추구하는 합법적 이익 (해당 시), RTX가 정보를 공유하는 수취인의 범주, 동의 취소 권리나 특정 데이터 사용 반대 권리 및 관찰 감독당국에 불만을 제기할 권리 등 개인에게 제공되는 선택권과 권리 (해당 시), 그러한 선택권 행사의 결과, 개인정보 보호에 관한 질문이나 불만이 있을 때 RTX에 연락하는 방법, 수집된 데이터의 보존 기간 (해당 시), 자동 의사결정에 관한 정보 (해당 시), RTX가 수집된 정보의 일부를 EU 밖에 있는 수취인과 공유할 가능성이 있다는 사실, RTX가 의도하는 데이터 보호 방법 (해당 시). 이 통지를 하는 것이 (해당 개인으로부터 직접 개인 정보를 수집하지 않아서) 불균형적인 부담을 주게 되는 특별한 경우, RTX는 신중히 고려한 후 개인에게 통지를 하지 않거나 통지를 지연하는 결정을 할 수 있다.

d) *자신의 개인 정보에 대한 프라이버시 권리 행사를 위한 개인의 합법적 권리를 존중한다.*

RTX는 개인이 자신의 개인 정보에 대한 접근 및 수정을 요구하도록 허용한다. 그러한 요구가 분명히 근거가 없거나 과도한 것이 아닐 경우, 본사 및/또는 해당 사업체는 합리적 기간 내에 그 요구를 따라야 한다. 본사 및/또는 해당 사업체는 요구가 분명히 근거가 없거나 과도한 내용임을 입증할 부담이 있다. 개인은 자신의 신분 증거를 제시하도록 요구받거나, 해당 법률이 허용할 경우 서비스 수수료가 부과될 수 있다.

개인은 자신의 개인 정보 처리를 반대하거나, 자신의 개인 정보 차단 또는 삭제를 요구할 수 있다. RTX는 그러한 요구를 따라야 한다. 다만 계약 의무, 감사 요건, 규제 또는 법률적 의무에 따라 또는 법적 클레임으로부터 회사를 방어하기 위해 필요한 경우에는 개인 정보를 보존할 수 있다. RTX가 개인 정보를 처리하지 못하도록 선택한 결과로서 발생할 수 있는 결과(예: 요청한 서비스를 RTX가 제공할 수 없거나 거래를 할 수 없음)를 해당 개인에게 통지한다. 또한 개인도 자신의 요청 결과에 관하여 통지를 받게 된다.

특정 연락을 받지 않는 것을 선택한 개인의 경우를 제외하고, RTX는 해당 법률에 따라 개인의 관심사에 따라 개인에게 연락을 하기 위해 개인 정보를 처리할 수 있다. RTX로부터 마케팅 통신문을 받고 싶지 않은 개인들에게는 추가적 광고 제공에 반대할 수 있도록 쉽게 접근 가능한 수단(예: 계정 설정, 이메일 지침, 통신문의 링크)을 제공해야 한다. 스팸 방지 규정의 적용에 관하여 궁금한 사항이 있으면 privacy.compliance@utc.com으로 연락할 수 있다.

RTX가 개인 정보를 바탕으로 개인에 관하여 자동으로 결정을 내릴 경우, 개인의 정당한 이익 보호를 위해 적절한 수단을 제공해야 하며, 그 예를 들면 결정 논리에 관한 정보 제공, 결정 내용을 검토할 기회 제공, 개인이 자신의 견해를 제공하도록 허용하는 것 등이다.

e) *적절한 기술적 조직적 보안 조치를 구현한다*

개인 정보의 무단 처리 또는 불법적 처리를 방지하고 개인 정보의 우발적 변경, 무단 공개나 접근, 손실, 훼손 또는 손상을 방지하기 위해 RTX는 해당 처리의 민감성과 위험성, 해당 개인 정보의 성격 및 해당 회사 정책을 고려하여 적절한 보안 조치를 구현해야 한다. 사업체는 강력한 정보 위반 사건 대응 플랜을 구현하거나 RTX의 정보 위반 사건 대응 플랜을 준수해야 하며, 이들 플랜은 실제 정보 위반에 대해 적절히 대응하고 시정하는 내용이어야 한다.

RTX는 서비스 제공자들이 이들 BCR 또는 동등한 요구사항을 존중하도록 하고 RTX의 지침에 따라서만 개인 정보를 처리하도록 의무를 부과하는 서면 계약을 체결해야 한다. 서면 계약서는 RTX가 제공하는 표준 조건을 사용하거나, 또는 변경 사항은 지정된 사업부 개인정보 전문가, 교육을 받은 사업부 법률 고문 또는 RTX CPO의 승인을 받도록 해야 한다.

f) *적절한 보호 조치 없이 개인 정보를 EEA 및 스위스 밖의 제삼자나 서비스 제공자에게 전송해서는 안 된다.*

RTX 소속이 아니고 그리고 (1) (Directive 95/46/EC의 의미 내에서) 적절한 수준의 보호를 제공하지 않거나 (2) 승인된 구속력 있는 회사 규칙의 적용 대상이 아니거나 또는 (3) EU 적합성 요건을 준수하는 기타 약정을 맺지 않은 제삼자나 서비스 제공자에게 개인 정보를 RTX가 전송할 경우, 본사 및/또는 해당 사업체는 다음 조치를 취해야 한다.

- 제삼자의 경우: 본 BCR에 상응하는 보호 수준을 제공하는 모범 계약 조항이 포함된 적절한 계약적 통제 방식을 구현하거나 또는 전송이 (1)

개인의 명확한 동의 하에 이루어지거나 (2) 개인과 체결할 계약 체결 또는 이행을 위해 필요하거나 (3) 중요한 공공 이익을 근거²로 필요하거나 법적으로 필요하거나 (4) 개인의 중요한 이익을 보호하기 위해 필요하거나 또는 (5) 법적 클레임의 규명, 행사 또는 방어를 위해 이루어지도록 보장해야 한다.

- 처리 업체의 경우: 본 BCR에 상응하는 보호 수준을 제공하는 모범 계약 조항이 포함된 적절한 계약적 통제 방식을 구현해야 한다.

g) *적절한 책임 조치 시행*

'EU 일반 정보 보호 규정' 및 영국 법규에 따라 개인 정보에 대한 데이터 통제자 또는 처리업체 역할을 수행하는 사업체는 책임 요건을 준수해야 하며, 그 예로서 처리 작업을 기록한 개인 정보 데이터 인벤토리를 유지하고, 데이터 보호 영향 평가를 수행하고, '일반 정보 보호 규정'의 요구에 따라 계획적, 기본적으로 개인정보 보호 원칙을 이행해야 한다. EU 개인 정보와 관련된 모든 개인 정보 데이터 인벤토리는 '일반 정보 보호 규정'의 요건에 따라 요구할 경우 관할 감독 당국에 제공해야 한다.

2. **거버넌스:** RTX는 BCR 준수를 보장할 수 있는 거버넌스 인프라를 유지하기 위해 최선을 다하고 있다. 이러한 인프라의 구성 요소는 다음과 같다.

a) **윤리준법 책임자("ECO"):** BCR 준수를 촉진하며, BCR 관련 내부 의견 및 불만을 수렴하는 내부 연락처 역할을 수행한다. RTX는 윤리준법 책임자가 프라이버시 불만의 접수 및 조사, 프라이버시 우려사항의 해결 지원, 필요 시 불만 사항의 검토 및 해결을 위해 불만 내용을 해당 담당자(개인정보 전문가 또는 개인정보실 등)에게 전달하는 교육을 받도록 해야 한다.

b) **옴부즈맨 프로그램:** 옴부즈맨 프로그램에 소속된 개인들은 BCR과 관련된 내부 및 외부 의견과 불만을 접수하는 방안을 유지해야 한다. RTX의 옴부즈맨 프로그램은 개인, 서비스 제공자 및 제삼자가 지침을 구하고, 질문하고, 의견을 제시하고 부당행위 의심 사례를 보고할 수 있는 안전하고 비밀이 유지되는 채널을 제공한다. 옴부즈맨 프로그램은 불만 제기자가 동의할 경우

² 해당 법률에 따라 사업체는 민주 사회에서 국가/공공의 안전, 국방, 형사 범죄의 예방, 조사, 탐지 및 기소를 위해, 그리고 국제/국내 협약서에 명시된 제재 조치의 준수를 위해 필요할 경우 개인 정보를 법집행 당국 또는 규제 당국과 공유할 수 있다.

필요 시 검토 및 해결을 위해 불만 내용을 해당 개인정보 전문가나 개인정보실 등 담당자에게 전달한다.

- c) **개인정보 전문가:** 각 사업체는 적어도 한 명의 개인정보 전문가와 사업부의 다른 직원을 지정해서 개인정보 관련 문제와 관련하여 윤리준법 책임자를 지원하도록 한다. 개인정보 전문가는 경영진이 현지에서 BCR을 준수를 보장하고 사업부 내에서 결점을 파악하여 시정하는 업무를 지원한다. RTX는 개인정보 전문가가 해당 역할을 수행하는 데 필요한 충분한 자원과 독립적 권한을 갖도록 보장한다.
- d) **정보보호책임자 (“DPO”):** DPO의 역할은 해당 법률에 정의되어 있다. 해당 법률에서 요구할 경우 DPO를 지명한다. DPO는 정기적으로 RTX CPO와 협조한다.
- e) **개인정보 자문 위원회 (“PAC”):** PAC는 BCR 이행을 포함하여 RTX의 개인정보 준수 프로그램을 전반적으로 감독할 책임이 있다. PAC는 각 사업부를 대표하는 개인정보 전문가, 인사부(HR), 디지털/정보 기술(IT), 국제 무역 준법(ITC), 환경 보건 안전(EH&S), 재무, 공급 관리 및 RTX EU 부문의 대표들로 구성된다. 필요 시 여타 구성원을 임시로 또는 영구적으로 추가할 수 있다. PAC는 RTX CPO 및 개인정보실과 협조하여 글로벌 준법 계획 이행 방안을 개발하여 확실히 시행하고 보장 및 감사팀의 조사 결과에 대응해야 한다.
- f) **RTX 최고 개인정보 보호 책임자(CPO):** CPO는 개인정보 전문가들과 협조하여 BCR을 배포하고 이를 효율적 효과적으로 이행하도록 보장해야 한다. 또한 CPO는 정보 보호에 관한 교육 및 인식 제고 캠페인, 개인정보 전문가 지원 및 그들에 대한 교육을 책임지고 아울러 독점 정보 보호에 대한 기본 요구사항 외에도 정보 보호 요건의 존재와 목적을 촉진해야 한다. CPO는 개인정보 자문 위원회에 지침을 제공하고 주도해야 한다. CPO는 본사의 최고 개인정보 전문가 역할을 수행한다.
- g) **개인정보실(Privacy Office):** 개인정보실은 CPO, 개인정보 전문가, 지명된 정보보호 책임자 및 사업체 또는 본사에서 지명한 추가 인원으로 구성된다. 개인정보실은 PAC에 참여하고, 개인정보실이나 옴부즈맨 직원에게 접수되는 의견이나 불만에 대응하여 해결하고, ECO가 ECO팀에 접수되는 의견이나 불만에 대응하고 해결하는 업무를 지원한다.
- h) **RTX EU:** RTX EU는 자체 개인정보 전문가나 DPO를 통해 PAC에 참여한다. BCR 위반 증거가 있을 경우, PAC나 CPO가 RTX EU에 그 내용을 통지하고 RTX EU와 협의를 통해 적절한 시정 절차를 이행하기 위해 본사 및/또는 해당

사업체 및 개인정보 전문가와 협력한다.

3. **교육훈련:** RTX는 아래 범주에 속하는 사람들이 정보 보호, 보안, 스팸 방지 규정에 관하여 연례 교육을 받도록 해야 한다.

- 윤리준법 책임자
- 개인정보 전문가
- 직무의 중요한 부분으로서 개인의 개인 정보를 취급하는 직원 및
- 개인 정보 처리에 사용되는 도구 개발에 참여하는 직원.

4. **모니터링 및 감사:** RTX 부사장과 내부 감사부를 감독하는 내부 감사는 본 BCR 준수 상태를 평가하고 확실히 시정 조치를 취하도록 사업체를 후속 관리하기 위해 정기적인 보증 및 감사 프로그램을 운영한다. 부사장과 내부 감사는 내부 감사부 직원, CPO 및 사업체의 도움을 받아 본 BCR을 반드시 준수해야 하는 시스템과 프로세스에 대응하기 위해 BCR 감사 프로그램의 적절한 범위를 결정한다.

BCR 준수 감사 결과는 CPO에 통보하고 여기서 다시 RTX 부사장, 글로벌 윤리준법 책임자, RTX EU 및 개인정보 자문 위원회에 통보한다. RTX 부사장, 글로벌 윤리준법 책임자 또는 해당 지정인은 BCR 관련 자료 감사 결과를 RTX 본사 이사회 또는 이사회 위원회(예: 감사위원회)에 전달해야 한다. 요구가 있을 경우 EEA 및 스위스의 해당 정보보호 당국이 BCR 관련 감사 결과에 대한 접속 권한을 받을 수도 있다.

5. **권리 요구 및 불만 사항 처리:** 자신의 개인정보 처리에 관한 개인의 요구에는 아래와 같이 대응한다. 이 연락 방법은 현지 법률에 따라 보충할 수 있다.

a) **내부 - RTX 인트라넷에 접근이 가능한 사람의 요구**

RTX의 직속 직원인 사람은 요구 및 불만 내용을 해당 현지 인사부 담당자에 제출할 수 있다. 직원을 포함한 모든 사람들이 해당 현지, 지역 또는 글로벌 윤리준법 책임자("ECO")(옴부즈맨 프로그램 또는 개인정보실에 연락할 수 있다. 이들 담당자에 대한 연락 방법은 다음과 같다.

현지 HR	정규적인 내부 채널을 사용하여 연락함
ECO	http://ethics.utc.com/Pages/Global%20Ethics%20and%20Compliance%20Officers.aspx
옴부즈맨	인터넷: Ombudsman.confidential.utc.com

	<p>전화: 미국, 캐나다, 푸에르토리코 내에서는 전화 800.871.9065번을 이용한다. 미국 밖에서 전화할 때에는 여기에 있는 해당 AT&T 직접 접속 코드를 먼저 누른 후, 안내(음성 또는 톤)에 따라 옴부즈맨 무료 전화 번호를 누른다.</p> <p>우편: United Technologies Corporation, Attention: Ombudsman Program 10 Farm Springs Road, 10FS-2 Farmington, CT 06032-2526 USA</p>
개인정보실	privacy.compliance@rtx.com

HR, ECO 또는 개인정보실에 제출된 불만 사항: 이 불만은 필요 시 해당 개인정보 전문가 또는 CPO(또는 지정인)의 지원을 받아 불만 접수 그룹(HR, ECO 또는 개인정보실)에서 대응한다.

옴부즈맨 프로그램에 제출된 프라이버시 불만 사항: 불만을 제기한 사람이 추가적인 대응을 원하고 동의할 경우 불만 사항을 개인정보실로 전달하여 대응하고 해결하도록 한다.

b) 외부 - 여타 모든 개인의 요구

여타 모든 개인으로부터 접수된 요구와 불만 사항은 옴부즈맨 프로그램 또는 개인정보실로 보낼 수 있고 연락 방법은 다음과 같다.

옴부즈맨	<p>인터넷: Ombudsman.confidential.utc.com</p> <p>전화: 미국, 캐나다, 푸에르토리코 내에서는 전화 800.871.9065번을 이용한다. 미국 밖에서 전화할 때에는 여기에 있는 해당 AT&T 직접 접속 코드를 먼저 누른 후, 안내(음성 또는 톤)에 따라 옴부즈맨 무료 전화 번호를 누른다.</p> <p>우편: United Technologies Corporation, Attention: Ombudsman Program 10 Farm Springs Road, 10FS-2 Farmington, CT 06032-2526 USA</p>
개인정보실	privacy.compliance@utc.com

불만을 제기한 사람이 추가적인 대응을 원하고 동의할 경우, 옴부즈맨 프로그램에 제출된 불만 사항을 개인정보실로 전달하여 대응하고 해결하도록 한다.

c) 불만 처리에 관한 추가 정보

전체적인 구조적 결점을 나타내는 불만사항 및 감사 결과는 CPO가 PAC를 통해 대응함으로써 RTX EU 및 현지 개인정보 전문가와 협의하여 확실하게 글로벌 해결책을 마련한다.

불만 제기자에게 만족스럽게 불만을 해결할 수 없을 경우 현지 HR, ECO 또는 개인정보 전문가가 그 문제를 CPO에게 보고한다. 그러면 CPO는 이용 가능한 불만 처리 절차를 통해 해결할 수 없는 모든 불만 사항을 RTX EU에 통보한다.

RTX는 요구/불만을 접수한 후 5 근무일 내에 초기 대응을 하기 위해 노력하고 있다. 요구/불만의 복잡성과 범위에 따라 그 기간이 길어질 수 있지만 1개월을 초과해서는 안 된다.

BCR의 어떠한 조항도 EEA 또는 스위스에 있는 사업체의 해당 법률 위반과 관련하여 개인이 해당 현지 법률에 따라 불만 사항을 관할 정보보호 당국이나 법원에 제출할 권리에는 영향을 주지 않는다.

6. **개인의 집행 권리 및 보증:** 개인은 본 섹션과 섹션 B, C, D.1, D.5, D.7, D.8, D.9에 따라 명시적으로 부여되는 권리 혜택 그리고 본 섹션에서 RTX EU가 보증하는 혜택을 받는다.

본 BCR 위반 혐의가 있을 경우 유럽 연합, 영국 또는 스위스 거주자인 개인은 다음을 수행할 수 있다.

- 개인의 상시 거주지, 근무지 또는 침해 혐의 장소가 속한 EU 회원국의 데이터 보호 당국에 불만을 제기하거나, 또는
- 통제자 또는 처리업체의 사업장이 있거나 또는 개인의 상시 거주지가 있는 곳의 EU내 관할 법원 중에서 선택하여 소송을 제기할 수 있다.

본 BCR에 근거하여 달리 권리를 보유한 모든 개인들(유럽 연합, 영국, 스위스 거주자가 아닌 개인 포함)은 자국법률에 따라 법적 배상 절차를 진행할 수 있다.

RTX 본사의 지원을 받아 RTX EU는 (1) EEA 밖에 있는 RTX 본사나 사업체에 의한 위반을 시정하고 (2) EEA 및 스위스 밖에 있는 본사 및/또는 사업체의 BCR 위반 결과에 따른 손해에 대해 본 섹션에 언급된 법원이 판결한 보상금을

개인에게 지급하도록 확실히 조치를 취하도록 할 책임이 있다. 다만 해당 사업체가 이미 보상금을 지급했거나 명령을 준수한 경우는 그에 따른다.

개인이 손해를 입었음을 입증할 수 있을 경우, RTX 본사와 협조하여 해당 본사 및 사업체가 BCR에 근거한 의무를 위반하지 않았음을 증명하는 것은 RTX EU의 책임이다. 그러한 증거를 제시할 수 있을 경우 RTX EU는 BCR에 근거한 책임을 면할 수 있다.

유럽 경제 지역이나 스위스에서 직접 또는 간접적으로 발생하지 않은 개인 정보와 관련하여 EEA 나 스위스 밖에 있는 사업체의 위반 행위를 시정하기 위해 확실한 조치를 취하도록 할 책임은 RTX 본사에 있다.

본 BCR을 개인정보 전송 위해 합법적 문서로 간주하는 EEA 회원국 및 스위스를 제외한 국가들의 경우, 그러한 국가의 개인들은 섹션 D. 1, D. 5, D. 7, D. 9에서 명시적으로 부여하는 권리 혜택을 받는다. 따라서 이들 국가의 해당 개인들은 자신의 국가에서 BCR 위반 사업체에 대해 해당 조항을 집행하기 위해 원하는 조치를 취할 수 있다.

7. **정보보호 당국과의 협조:** 사업체는 BCR과 관련된 질문 및 확인과 관련하여 해당 정보보호 당국이 합리적으로 요구하는 지원을 제공해야 하며 여기에는 요구 시 감사 결과를 제공하는 것도 포함된다.

RTX는 해당 EEA/스위스 정보보호 당국의 최종 결정을 준수해야 하며, 그 결정에 대해서는 추가로 이의신청을 할 수 없고 또는 이의신청을 하지 않는다는 RTX의 결정도 준수해야 한다. RTX의 BCR 준수 상태를 관할 정보보호 당국이 해당 법률에 따라 감사할 수 있다는 점을 RTX는 인정한다.

8. **BCR의 변경:** 명시된 보호 수준을 중대하게 변경하는 BCR 변경 또는 개정이 있을 경우 RTX EU는 신속히 그 내용을 벨기에 정보보호국에 통보해야 하고, RTX EU는 일년에 한번씩 전년도에 발생한 모든 변경 사항을 벨기에 정보보호국에 통보해야 한다.

RTX EU는 그룹간 계약을 체결했던 모든 사업체의 최신 목록과 모든 BCR 갱신 최신 목록을 유지해야 한다. 이 목록은 요구가 있을 경우 적용 대상 사업체, 개인, EEA/스위스 정보보호 당국에 제공해야 한다. RTX EU는 어떠한 경우에도 회사 규칙 계약을 체결했던 모든 사업체의 최신 목록 사본을 적어도 일년에 한 번씩 벨기에 정보보호국에 제공해야 한다.

RTX는 해당 그룹 구성원이 그룹간 계약을 체결한 후 준수할 수 있을 때까지는 본 BCR에 의존해서 개인 정보를 RTX 그룹의 여타 구성원에게 전송해서는 안 된다.

9. **본 BCR 알림:** 개인들이 본 BCR에 근거한 자신의 권리를 알 수 있도록 EEA 및 스위스에 있는 사업체들은 자사의 대외 웹사이트에 본 BCR을 게시하거나 링크를 유지해야 한다. RTX는 www.utc.com 또는 대체 웹사이트에 본 BCR을 게시하거나 링크를 유지해야 한다.

별첨 A – 용어 정의

"사업부"란 RTX의 주요 부분으로서 수시로 변경될 수 있으며, 현재는 Collins Aerospace, Digital and Global Business Systems, Integrated Defense and Missile Systems("IDMS"), Intelligence, Space and Airborne Systems("ISAS"), Pratt & Whitney, RTX Research Center 및 RTX 본사로 구성된다.

"RTX 본사"란 미국에 있는 회사의 본사를 말한다. 주소: 870 Winter Street, Waltham, MA 02451.

"정보 위반"(Data Breach)이란 암호화되지 않은 개인 정보 또는 암호화된 개인 정보를 무단으로 획득 또는 사용하는 것을 의미하며, 비밀 프로세스나 키가 훼손되었을 경우 개인 정보의 보안, 비밀 또는 무결성을 훼손하여 한 명 이상의 개인에게 상당한 위협을 야기할 수 있는 상황을 말한다. 위협에는 신분 도용 가능성, 곤란한 상황, 개인 정보의 공개 또는 기타 부정적 영향 등이 포함된다. RTX나 그 직원 또는 서비스 제공자가 합법적 목적으로 선의이지만 무단으로 개인 정보를 획득할 경우, 개인 정보를 무단으로 사용하거나 추가적인 무단 공개가 발생하지 않는 한 보안 정보 위반으로 간주하지 않는다.

"개인"이란 직원, RTX 고객이나 공급자, RTX 제품 및 서비스의 소비자인 자연인을 의미한다.

"사업체"(Operating Businesses)는 위치 불문하고 RTX 및 모든 사업 부문, 부서, 본부 및 기타 모든 운영 업체(RTX가 지배 지분 또는 효율적 경영 통제권을 가진 통제 대상 합작 투자회사, 파트너십 및 기타 사업체 등 포함)를 의미하며, 다만 본사는 제외된다.

"개인 정보"란 식별된 또는 식별 가능한 자연인과 관련된 정보를 의미한다. 이는 특히 신분증 번호, 이름 또는 사람의 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특유한 하나 이상의 요소 등 식별자를 언급하여 직접 또는 간접적으로 식별된 또는 식별 가능한 자연인에 관한 정보이다. 개인이 식별 가능한지 여부는 RTX나 다른 사람이 해당 개인을 식별하기 위해 사용할 것으로 합리적으로 예상되는 수단에 따라 다르다. 그러한 수단이 사용될 가능성이 없거나 식별이 불가능할 경우 해당 데이터는

익명이며 본 BCR의 적용 대상이 아니다. 이 용어에는 민감한 개인 정보도 포함된다. 개인 정보에는 매체 불문하고 하드 카피, 전자식, 비디오 녹화, 오디오 녹음 등으로 수집, 처리, 전송되는 정보가 포함된다.

"직원"이란 RTX의 종업원을 의미하며 여기에는 RTX 이사, 임원, 임시직, 계약자, 도급 근로자 RTX가 소유하는 계약 근로자가 포함된다.

"프로세스"란 자동 수단 여부에 관계 없이 개인 정보에 대해 수행하는 작업 또는 일련의 작업을 의미하며 여기에는 수집, 기록, 조직, 저장, 각색 또는 변경, 조회, 참고, 사용, 전송을 통한 공개, 이전 또는 유포, 기타 방식의 제공, 정렬 또는 조합, 차단, 삭제 또는 파괴 작업이 포함된다.

"민감한 개인 정보"는 개인 정보의 하위 집합으로서 인종 또는 민족적 출신, 정치적 의견, 종교적 또는 철학적 신념, 노동 조합 가입, 건강, 성적 선호도, 성 생활 또는 범죄 행위나 범죄 행위 주장 및 처벌 가능성 등과 관련하여 식별된 또는 식별 가능한 사람과 관련된 정보를 의미한다.

"서비스 제공자"는 RTX에 대한 직접적 서비스 제공을 통해서 RTX가 보유한 개인 정보를 처리하거나 달리 접근하도록 허용된 업체나 사람을 의미한다.

"제삼자"란 회사 규칙 계약을 체결한 개인이나 업체(RTX 본사 및 사업체는 제외) 및 그들의 직원과 서비스 제공자를 의미한다.

"RTX"란 RTX의 본사 및 사업체를 의미한다.

별첨 B - 내부 처리 조항

이 조항은 BCR의 구속을 사업체(이하 "RTX 본인")가 프로젝트를 해당 개인 정보 처리업에 종사하는 다른 구속 받는 사업체(이하 "RTX 처리업체")에 위탁할 때 적용한다. RTX 본인과 RTX 처리업체 간에 작업 지시서가 수반되는 프로젝트인 경우, 작업 지시서에는 내부 처리 조항의 조건 "본 작업 지시서에 명시된 서비스는 개인 정보 보호를 위해 RTX BCR에 명시된 내부 처리 조항의 적용을 받는다"는 내용을 언급해야 한다.

이 조항에 정의된 용어들은 RTX BCR에 정의된 용어를 참조한다.

1. RTX 본인과 RTX 처리업체는 전체 작업 지시서 기간 동안 계속 RTX BCR의 구속을 받는다는 점에 동의한다. 이 조항은 작업 지시서 기간 동안 적용한다. 본

조항의 섹션 4.2, 4.4, 4.5, 4.8, 4.10, 4.11의 규정은 작업 주문서 해지 후에도 계속 유효하다.

2. RTX 처리업체는 서비스를 수행할 때 RTX 본인을 대신하여 개인 정보를 처리한다.

3. RTX 본인의 의무:

3.1. RTX 본인은 RTX 처리업체에게 해당 개인 정보의 성격과 목적, 처리 기간에 관하여 명확한 지침을 제시해야 한다. 이 지침은 RTX 처리업체가 본 조항 및 RTX BCR의 의무를 충족할 수 있도록 충분히 명확해야 한다. 특히 RTX 본인의 지침은 하도급 업체의 사용, 개인 정보의 공개 및 RTX 처리업체의 기타 의무에 적용될 수 있다.

3.2. RTX 본인은 본 조항에 따라 RTX 처리업체가 수행할 처리와 관련된 국가 정보 보호법 및 관련 법률 문서, 규정, 명령 및 유사 문서에 대한 모든 변경 내용을 RTX 처리업체에 알리고, RTX 처리업체가 그 변경 내용을 준수하는 방법에 관한 지침을 제시해야 한다.

4. RTX 처리업체의 의무

4.1. RTX 처리업체는 작업 지서에 명시된 또는 서면으로 통지하는 RTX 본인의 지침에 따라 개인 정보를 처리해야 한다. RTX 처리업체는 다른 목적이나 다른 방식으로 해당 개인 정보 처리를 수행해서는 안 된다.

4.2. RTX 처리업체는 RTX BCR의 모든 조항 특히 섹션 D.1.e.를 준수해야 한다.

4.3. RTX 처리업체는 RTX 본인의 사전 서면 승인 없이 본 조항의 섹션 4.6에 근거한 하위 처리업체 이외의 제삼자에게 해당 개인 정보를 공개하거나 전송해서는 안 된다.

4.4. RTX 처리업체가 RTX BCR (섹션 D.1.f.)에 따라 유효한 법적 의무의 결과로서 처리를 수행하는 것이 필요할 경우, 본 섹션 4의 요건에도

불구하고 처리를 수행해야 한다. 이 경우 RTX 처리업체는 그러한 요구사항을 준수하기 전에 RTX 본인에게 사전 서면 통지를 해야 하며, 다만 해당 법률, 규정 또는 정부 당국이 통지를 금지할 경우는 그에 따르며, 그러한 공개와 관련하여 RTX 본인의 모든 합리적 지시를 준수해야 한다.

- 4.5. RTX 처리업체는 개인으로부터 자신의 개인 정보와 관련된 권리 행사에 관하여 받은 통신문을 3영업일 내에 RTX 본인에게 통지해야 하고, 그 통신문에 대응한 RTX 본인의 모든 지침을 준수해야 한다. 또한 RTX 처리업체는 개인으로부터 자신의 개인 정보에 대한 개인 권리와 관련하여 받은 통신문에 대응하기 위해 RTX 본인이 요구하는 모든 지원을 제공해야 한다.
- 4.6. RTX 처리업체는 작업 지시서에 근거한 의무 이행을 지원 받기 위해 하위 처리업체를 고용할 수 있다. 다만 RTX 본인으로부터 사전 서면 승인을 받아야 한다. RTX 처리업체는 모든 측면에서 본 조항에 근거하여 RTX 처리업체에 부과되는 의무에 버금가는 의무를 하위 처리업체에 부과하는 서면 계약을 하위 처리업체와 체결해야 한다. RTX 처리업체는 RTX BCR 섹션 D.1.f를 준수해야 한다.
- 4.7. RTX 처리업체는 자사에 적용되는 정보보호 법률(또는 기타 법률이나 규정)의 어떤 내용도 본 조항에 근거한 자신의 의무 이행을 방해하지 않는다는 점을 진술하고 보증한다. 그러한 법률이 변경되어 RTX 처리업체의 본 조항 준수에 중대하게 부정적 영향을 줄 가능성이 있을 경우 또는 RTX 처리업체가 달리 본 조항을 준수할 수 없을 경우 RTX 처리업체는 15 영업일 내에 RTX 본인에게 통지해야 하고 RTX 본인은 해당 작업 지시서를 즉시 해지할 권리를 갖는다.
- 4.8. RTX 처리업체는 RTX 본인이 RTX BCR 섹션 D.4에 따라 RTX 처리업체의 본 조항 준수 상태를 감사하도록 요구할 수 있다는 점에 동의한다. 특히 RTX 처리업체는 그러한 의무 준수를 입증하기 위해 필요한 모든 정보를 RTX 본인에게 제공해야 하고, RTX 본인이 또는 그의 위임을 받은 감사인이 수행하는 검사를 포함하여 모든 감사를 받아야 한다.
- 4.9. RTX 처리업체는 RTX 처리업체의 권한 하에 개인 정보를 처리하는 모든 사람이 해당 기밀유지 의무의 적용을 받도록 해야 한다.

- 4.10. RTX 처리업체는 RTX 본인이 해당 데이터 보호 법률의 의무를 준수하도록 지원해야 하고, 해당 시 데이터 보호 영향 평가를 수행하는 것도 지원해야 한다.
- 4.11. RTX 처리업체는 데이터 위반 발생 시 RTX에 지체 없이 통보해야 하고, 데이터 위반을 시정하고 재발 방지를 위해 신속히 조치를 취하고, 필요 시 RTX가 그 조치를 수행하도록 지원해야 한다. RTX 또는 해당 사업체는 적절한 조사 및 시정과 관련하여 RTX 본인 및 RTX 처리업체와 협조해야 한다. 또한 RTX 처리업체는 필요 시 RTX 본인이 데이터 위반에 관하여 정부 당국이나 해당 개인들에게 통보해야 하는 본인의 의무를 이행하도록 지원해야 한다.
5. 작업 지시서가 해지될 경우, RTX 처리업체는 보유 중인 모든 해당 개인 정보를 매체 불문하고 모든 데이터 사본과 함께 RTX 본인에게 송부하거나 파괴해야 한다. 다만 해당 법률, 규정 또는 정부 당국이 RTX 처리업체에게 개인 정보나 그 일부를 보유하도록 요구할 경우는 그에 따른다. 이 경우 RTX 본인에게 그 의무를 신속히 통지해야 한다.
6. 이 조항은 RTX 본인이 설립된 국가의 법률의 적용을 받고 그에 따라 해석한다. RTX BCR 섹션 D.6의 규정을 침해하지 않음을 전제로, 본 조항의 각 당사자는 RTX 본인 국가의 법원이 본 조항과 관련하여 발생하는 클레임이나 사항에 대해 배타적 관할권을 갖는 것에 취소 불가능하게 따른다.
7. 기타 사항.
- 7.1. 본 조항의 규정들은 분리할 수 있다. 임의 절이나 조항의 전부 또는 일부가 무효 또는 집행 불가능하게 될 경우 해당 무효 또는 집행 불가능성은 해당 절이나 조항에만 영향을 주며 본 조항의 잔여 항목은 완전한 효력을 유지한다.
- 7.2. 본 조항의 규정들은 RTX 본인 및 RTX 처리업체와 그들 각각의 승계인 및 양수인에게 이익이 되고 구속력을 갖는다.