경영유의사항 등 공개안

1. 금융회사명 : ㈜비바리퍼블리카(이하 '토스'라 함)

2. 제재조치일 : 2024.10.25.

3. 조치내용

대 상	내 용
기 관	경영유의사항 2건, 개선사항 18건

4. 제재대상사실

가. 경영유의사항

(1) 마이데이터 서비스 및 업무처리 절차에 대한 점검 강화

토스는 마이데이터 서비스 보안성 확보를 위해 자체전담반을 구성하여 앱, 네트워크, 서버 등에 대한 디버깅공격, 입력 값 검증 등 기술적인 보안 취약점 점검을 수행하고 있으나

마이데이터 서비스의 각 단계별 기능*이 마이데이터 가이드라인 등에 따라 적절히 구현되었는지 여부와 업무처리과정에서 담당 직원이 관련 내규**를 준수하는지 여부를 점검하는 절차가 마련되어 있지 않아

* 고객의 마이데이터 서비스 가입, 통합인증, 본인신용정보 전송 등
** 「내부관리계획」 제16조(개인신용정보 처리기준)

마이데이터서비스 시범운영기간(2021.12.18.~12.29.) 중 본인신용정보의 정기적 전송(주기 포함)을 필수사항*으로 동의받아 이를 선택사항으로 변경하여 재동의 받은 사례가 있으므로

* 「금융분야 마이데이터서비스 가이드라인(2021.7월, 금융위)」의 본문 "3.4. 전송요구 방법 및 절차" 및 부록 2. "본인인신용정보관리회사 전송 표준전송요구 및 표준동의서([통합인증양식 1번]표준 전송요구서의 가입상품 목록 전송요구서)"에서는 본인신용정보의 정기적 전송 여부와 전송 주기를 고객이 선택할 수 있도록 안내

업무 담당직원이 관련 내규, 가이드라인 등을 충분히 이해하고 업무를 수행할 수 있도록 업무처리 절차를 강화하고, 내규 등의 준수 여부를 확인하기 위한 정기적인 점검절차를 마련할 필요가 있음

(2) 감사위원회 운영 및 내부감사 기능 강화

정관 제25조 및 제33조 등에 의하면 회사는 감사위원회를 구성하여 회사의 회계 및 업무에 대한 감사를 수행하도록 정하고 있는데도

검사종료일(2022.4.15.)까지 감사위원회는 구성되어 있으나 감사위원회 운영 및 감사업무 수행을 위한 조직, 감사규정이 마련되어 있지 않아 일부 회계 부문에 대해서만 감사를 수행하고 업무 전반에 대한 내부감사 실적이 없으며,

또한, 내규 등에 일상감사, 정기감사 및 특명감사 등의 내부감사 절차가 없는 등 임직원의 직무수행 관련 적법성 및 타당성 등에 대한 감사 활동*이 원활히 작동하지 않고 있으므로

* GRC팀(Governance, Risk, Compliance)에서 내부통제 기획 및 임직원 법규준수 교육을 실시하는 등 준법감시 기능은 작동하고 있으나, 업무 전반에 대한 내부감사 기능은 취약한 수준

감사업무의 권한, 책임, 구성 등에 관한 내용이 포함된 감사위원회 운영 및 회사 업무 전반에 대한 내부감사 수행을 위한 제규정을 제정·운용하는 한편,

내부감사 및 감사 결과 조치 등의 사후관리 업무가 실효성 있게 수행될 수 있도록 내부감사 조직을 신설하고 전문인력을 배치·양성하는 등 감사위원회 운영 및 내부감사 기능을 강화할 필요가 있음

나. 개선사항

(1) 개인신용정보 이용 및 제공 내역의 조회·통지 절차 등 개선

토스는 「신용정보법」 제35조 및 동법 시행령 제30조 제1항 등에 따라 신용정보주체가 개인신용정보 이용 및 제공 내역을 조회할 수 있도록 토스 앱(App) 내 고객센터 또는 유선 고객지원센터를 통해 고객의 조회요청을 접수하고, 내부 절차에 따라 그 내용을 통지하고 있으나

동 조회·통지 절차가 자동화되지 않고 업무매뉴얼 등 공식적인 문서가 마련되어 있지 않아, 실제 고객이 개인신용정보 이용 및 제공 내역의 조회를 요청하더라도 통지절차를 누락할 우려가 있으므로

토스 앱(App) 및 홈페이지 내 개인신용정보 이용 및 제공내역 조회를 신청하고 이를 확인할 수 있는 기능을 추가하여 신용정보주체가 개인신용정보 이용 및 제공 내역을 쉽고 편리하게 조회할 수 있도록 개선하고 동 서비스 이용방법 등을 토스 앱(App) 등에 게시할 필요가 있음

또한, 토스 앱(App) 및 홈페이지 내 게시된 개인정보처리방침을 통해 '개인신용정보 이용 및 제공 내역 통지 요구'를 할 수 있다는 사실과 요청 방법에 대하여 안내하고 있으나, 통지 주기 및 수수료 금액에 대해서는 안내하지 않고 있으므로 이를 개선할 필요가 있음

(2) 개인신용정보 수집·이용 동의시 법정 고지사항 안내 절차 개선

토스는 개인신용정보를 수집하고 이를 활용하기 위하여 토스 앱(App) 또는 홈페이지 회원 가입시 개인신용정보 수집·이용 동의서를 통해 법정 고지사항*을 안내하고 신용정보주체로부터 동의를 받고 있으나,

* 개인신용정보 수집·이용 목적, 수집 항목, 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의거부에 따른 불이익이 있는 경우 그 내용(「신용정보법」 제34조의2 제1항)

각 수집·이용 목적별 개인신용정보 항목에 대한 보유 및 이용기간을 일괄적으로 표시하고 동의 거부권에 대한 내용을 명확하게 기재하지 않는 등 고지 내용이 미흡하여, 신용정보주체가 수집·이용 목적별로 개인신용정보의 보유 및 이용기간이 달라질 수 있고, 동의 거부권이 있다는 사실을 정확히 인지하지 못할 우려가 있으므로

신용정보주체가 개인신용정보 수집·이용 동의시 법정 고지사항의 내용을 명확히 이해할 수 있도록 동의서 양식을 개정하는 등 관련 업무를 개선할 필요가 있음

(3) 내규관리 절차 개선

회사는 IT 관련 21개 규정·지침과 21개 매뉴얼·절차서를 마련하고 금융소비자 보호 업무 관련 5개 규정 및 지침을 운용하는 등 업무별로 필요한 내규를 운용중이나,

내규 전반에 대하여 제·개정 절차가 수립되어 있지 않고 내규별 관리 조직이 업무 소관별로 지정되어 있지 않으며,

IT개발, 대출·카드 모집 등 회사의 여러 업무에 대한 명문화된 규정이 마련되어 있지 않아 업무처리 절차의 적정성을 점검하기 어렵고 내규에 대하여 정기적인 개정 및 검토를 수행하지 않고 있으므로

내부 감사 조직에서 내규 제·개정 권한, 절차 등을 정하는 내규관리규정을 제정하고, 동 내규관리규정에 따라 IT개발 등 여러 업무에 대한 명문화된 규정을 마련하는 한편, 업무환경 변화에 따른 내규의 정기적인 검토 및 개정을 수행할 수 있도록 내규별 담당 조직을 명시적으로 지정하는 등 내규 관리 시스템을 구축하여 실효성 있는 내규 관리 체계를 마련하시기 바람

(4) 미성년자 선불지급수단 발급관련 법정대리인 검증절차 개선

회사는 만 14세 미만 미성년자를 대상으로 한 카드형 선불전자지급수단 발급 과정에서 법정대리인의 동의를 받고 성명·나이 등 기본 정보를 바탕으로 법정대리인의 대리권을 검증하고 있으나,

정당성 검증시 주민등록자료 등 별도 자료를 활용하지 않고 있어 카드 발급을 원하는 미성년자가 임의로 지정한 성인의 토스 앱(App)을 통해 동의가 되면 카드발급이 가능한 상태로 운영되고 있으므로

만 14세 미만 미성년자 대상 카드형 선불전자지급수단 발급 과정에서 법정대리인 동의 처리 시 본인 확인 절차를 강화하기 위해 행정안전부 주민등록 정보 자료* 등을 활용하여 법정대리인 동의 여부에 대한 검증 절차를 개선하시기 바람

* 법정대리인은 토스 앱(App)내 행안부 주민등록등본 발급 서비스 활용

(5) 광고 사전심의 절차 개선

회사는 내규 「광고업무지침」에 따라 회사의 금융상품판매대리·중개업자 업무 광고에 대하여 준법감시인의 사전 심의를 거치고 광고에 준법감시인의 심의필을 표시하도록 규정하고 있으나,

「광고업무지침」에서 금융상품판매대리·중개업자 업무 광고에 대한 구체적인 심의 기준과 절차를 마련하지 않고,

광고 매체로 게재하는 배너 광고 등 금융상품 광고에 대해서도 별도의 확인 절차가 마련되어 있지 않으므로

「금융광고규제 가이드라인」을 준수할 수 있도록 광고심의 체크리스트를 마련하고 심의 기준을 구체화하는 한편, 금융상품을 토스 앱(App)에 광고하는 것에 대한 점검 절차를 마련하시기 바람

(6) 소비자보호 총괄기관 독립성 제고

회사는 내규 「소비자보호규정」 및 「내부통제규정」등에서 GRC팀을 소비자보호 총괄기관으로 지정하고 상품 판매·개발 업무로부터 독립하여 운영중이나,

명문화된 보상체계나 인사 규정이 없고 회사 사업실적과 연동된 보상이나 평가 등으로 인해 소비자보호 업무시 이해 상충이 발생할 우려가 있으므로

소비자보호 총괄기관이 실효성 있는 소비자보호 업무를 할 수 있도록 구체적이고 명문화된 별도 평가(보상)체계를 마련하는 등 관련 업무를 개선하시기 바람

(7) 서비스 해지 등 업무의 고객 본인확인 절차 개선

회사는 고객이 고객센터를 통해 서비스 해지(선불잔액정산 등)를 요청하거나, 이상금융거래탐지시스템(FDS)에 의해 거래가 차단된 고객이 차단 해제를 요청하는 경우, 본인확인을 위해 인감증명서 또는 본인서명사실확인서를 징구하고 있어 과도한 고객의 불편을 초래하고 있으므로

고객 본인확인 절차 규정을 마련하고 인감증명서 또는 본인서명사실확인서를 징구하는 대신 비대면 실명확인 절차를 활용하는 등 고객 본인확인 절차를 개선하시기 바람

(8) 거래 종료된 이용자의 개인신용정보 관리업무 개선

회사는「정보보안규정」및「데이터 보유기간과 파기의 기준 및 절차」에 따라 거래 종료된 이용자의 신용정보를 분리보관 및 파기하고, 신용정보관리·보호인과 개인정보보호팀이 개인신용정보 파기 프로세스 및 결과를 관리·감독하고 있으나,

분리보관 및 파기에 대한 구체적인 실행방안이 마련되어 있지 않아, 파기업무가 일정한 주기로 시행되지 않고* 있으며, 이로 인해 신용정보가 법정기한**을 넘겨 파기될 가능성이 있고,

* '21년도 7차례(1월, 4월, 5월, 7월, 8월, 9월, 12월), '22년도의 경우 1차례(2월) 수행
** 상거래 종료 후 최대 5년 이내 삭제 필요

시스템에서 자동으로 수행되는 분리보관 작업의 적정성에 대한 확인 및 검증작업이 없어 시스템 오류 발생시 신용정보의 보안조치가 누락될 우려가 있으므로

신용정보보호·관리인은 상거래 종료된 신용정보에 대한 파기 등 보안조치가 실효성 있게 이루어지도록 관련 절차를 개선하시기 바람

(9) 신용정보 조회 적정성 점검 관리체계 개선

회사는 내규 「개인정보 및 신용정보 보호를 위한 내부관리계획」 및 「보안정책문서」에 따라 개인정보보호팀에서 개인신용정보취급자의 신용정보 조회목적 및 이력을 검토하고 신용정보 관리·보호인이 확인하고 있으나,

신용정보 조회목적의 분류가 세분화 되어 있지 않아 특정항목*의 비중이 대부분을 차지하고 있으며, 사후 적정성 확인을 위한 점검기준도 구체적이지 않아 내부통제 실효성이 떨어지고, 내규상 개인신용정보 오남용에 대한 직원 제재기준이 불명확하게 운영되고 있으므로

* '20.12월 한달 자료를 확인한 결과 '고객상담' 목적이 73.8% 차지

신용정보관리보호인은 개인신용정보 오남용 방지를 위해 개인신용정보 조회목적을 세분화하고 사후 적정성 점검기준을 마련하는 한편, 부당조회 등 개인신용정보 오남용 직원에 대한 제재기준을 마련하는 등 관련 업무를 개선하시기 바람

(10) 이용자로부터 수집하는 개인신용정보 동의방식 개선

회사는 이용자로부터 개인신용정보 수집 및 제3자제공 등의 동의를 받는 방법에 관하여 내부 지침*을 마련하여 운영하고 있으나,

* 내부 가이드라인 「개인정보 처리에 따른 동의 받는 방법」(개인정보보호법, 신용정보법 준용)

가이드라인 준수 여부에 대한 점검절차가 없어 가이드라인이 준수되지 않은 상태*로 신규 서비스가 출시되거나 개편될 우려가 있으므로

* 고객이 동의내용을 명확히 인지하지 못한 상태로 정보제공에 동의하는 경우 등

고객에게 동의내용을 명확히 알리고, 동의여부 의사표시를 확인하여 개인신용정보 수집 등을 진행할 수 있도록 가이드라인 준수 여부 점검 프로세스를 개선하시기 바람

(11) 모바일 앱(App) 화면 접근통제 개선

회사는 접근통제를 위해 앱(App)에서 송금 및 신용정보 조회시에는 핀(PIN) 번호 입력 등 추가 보안조치로 통제하고 있으나,

앱(App)에서 잔액현황 등 다른 금융정보 출력화면 접근시에는 별도의 보안 인증절차가 없어 스마트폰의 잠금기능 비활성화시 계좌 잔액 등이 화면에 노출될 우려가 있으므로,

고객이 앱(App) 첫화면에서 계좌 등 잔액 노출 여부와 앱 잠금설정 여부를 선택할 수 있는 권한을 고객에게 부여하고, 스마트폰 잠금 기능이 비활성화된 경우 앱(App) 잠금 기능을 활성화하는 등 보안조치를 개선하시기 바람

(12) 자료전송시스템 반출정책 개선

회사는 업무망에서 인터넷망으로 파일을 반출하기 위해 책임자 승인*을 받도록 운영하고 있으나,

* (개인정보 포함 파일) 개인정보보호담당자 1차 사전승인 → 자료전송시스템 관리자 2차 사후승인
(개인정보 미포함 파일) 자료전송시스템 관리자 사후승인

비밀번호가 설정된 파일은 개인정보 포함 여부를 확인하지 않아 개인정보가 포함된 파일이 책임자 검토 없이 외부로 반출될 수 있고,

업무와 무관한 자료전송시스템 관리자가 전체 반출파일에 대한 승인을 하고 있어 반출 사유의 적정성을 확인하기 어려우므로

비밀번호가 설정된 파일도 업무 관련 책임자가 개인정보 포함여부 등을 검토할 수 있도록 조치하고, 파일반출 승인은 업무 책임자가 승인할 수 있도록 반출통제 정책을 개선하시기 바람

(13) 데이터베이스 등 전산자료 백업·소산정책 개선

회사는 서버, 네트워크, 보안장비 등 정보처리시스템의 전산자료 중요도에 따라 백업·소산주기를 설정하여 소산을 수행하고 있으나,

전산원장을 보관하는 데이터베이스 등 전산자료에 대하여 실시간 복제방식*으로 소산을 수행하고 있어 대량의 데이터가 잘못 수정되는 등 데이터 오염이 발생할 경우 데이터 복구에 어려움이 있으므로

* 주전산센터에서 생성된 데이터를 주전산센터에 실시간으로 1차 백업하고 제2전산센터에 동일 데이터를 원격 소산하는 방식

백업자료에 대하여 별도 장소에 실시간 복제가 아닌 방식으로 추가 소산을 수행하고 주기적으로 검증하도록 개선하시기 바람

(14) IT감사업무 개선

회사는 내부감사지침에 따라 IT업무에 대한 적정성 및 준법성을 점검하기 위해 IT 보안감사인을 지정하여 IT감사 활동*을 수행하고 있으나,

* 전자금융기반시설 취약점 점검결과 보완조치, 분기별 취약점 스캔점검 등

정보처리시스템 보안 로그(이벤트) 및 각종 접근통제 시스템에서 기록하는 다양한 감사로그*에 대하여 위험성 및 적정성을 검토하고 있지 않으므로

* 클라우드시스템 접근 및 활동 내역, 접근통제시스템을 경유하지 않은 시스템 접근 이력, 전산원장 조회·변경 내역, 시스템 접근권한 부여내역 등

시스템 접근내역 및 보안 로그(이벤트) 등을 탐지·관리하는 모니터링 체계를 구축하고, 접근통제시스템의 감사로그에 대하여 주기적으로 위험성 및 적정성을 점검하도록 개선하시기 바람

(15) 대량 전산원장 변경통제 업무 개선

회사는 전산원장 변경이 필요한 경우 데이터베이스 접근통제시스템을 통해 전산원장 변경 전·후 데이터를 기록하고 책임자 승인을 받은 명령문만 실행되도록 통제하고 있으나,

일부 예외* 변경 건은 데이터베이스 접근통제시스템의 통제 없이 명령문에

대한 책임자 승인만 받는 결과, 승인 이후 수정된 다른 명령문이 실행될 우려가 있으므로

* 데이터베이스 데이터구조 변경 등 사유로 대량(약 1만건 이상)의 전산원장 변경으로 인해 접근통제시스템에 과부하가 생길 우려가 있는 경우

데이터베이스 접근통제시스템의 통제 예외 건에 대하여 실행된 명령문이 승인받은 명령문과 동일한지 확인하고 IT감사를 통해 해당 내역을 점검하도록 개선하시기 바람

(16) 프로그램 소스코드에 대한 배포 책임자 지정업무 개선

회사는 소스코드 수정·추가에 따른 프로그램 배포(적용)시 제3자 코드 검증을 거쳐 책임자에게 승인을 받도록 되어 있으나,

회사 관리책임의 계열사 공통 소스코드에 대하여 계열사 소속 책임자가 최종 배포 승인을 할 수 있도록 운영*하고 있어 소스코드 배포에 대한 책임소재가 불분명할 우려가 있으므로

* 소스코드 수정자, 리뷰자 : 토스 ↔ 배포 책임자 : ㈜토스뱅크

계열사 소속의 직원이 프로그램 수정·배포를 하는 경우 계열사 책임자가 1차 확인하고 토스의 책임자가 최종 승인하도록 절차를 개선하시기 바람

(17) 클라우드시스템 백업정책 개선

회사는 결재승인 등 대내·외 전자금융거래 관련 업무처리를 위해 클라우드 시스템(Slack*)을 이용중이고, 클라우드 서비스 업체에서 고객(토스)의 자료를 보호하기 위한 백업**을 수행하고 있으나,

* 대화방식의 업무소통을 지원하는 클라우드 기반 협업도구
** 클라우드 서비스 업체 측의 과실로 인한 데이터 손실을 방지하기 위해 업체 자체적 백업

회사 자체적으로 주요자료에 대한 백업은 수행하고 있지 않아, 회사측의 과실*로 인해 손실된 데이터는 복구가 어려울 가능성이 있으므로

* 회사 실수로 Slack내 중요파일을 삭제하는 경우, 현 계약상 Slack에서 복구 의무가 없음

클라우드시스템(Slack)에서 제공하는 기능이나 별도의 솔루션 이용을 검토하여 주요정보는 회사 내부에 백업하도록 개선하시기 바람

(18) 시스템 접속 등 권한관리시스템 승인·처리 방식 개선

회사는 보안정책 변경, 시스템 접속권한 처리 등 각종 시스템에 대한 이용자 계정 관리를 위해 권한관리시스템을 통한 책임자 승인 및 처리 내역을 관리하고 있으나,

권한관리시스템에서 시스템 권한 부여가 책임자 승인 전에 가능하도록 되어 있어 미승인자에게 권한이 부여*될 우려가 있으므로

* 2021.10.1.(DB에 승인·처리일을 적재하기 시작한 일자) ~ 2022.3.28. 기간 동안 권한처리 2,425건 중 1,246건(51.3%)이 책임자 승인 전에 권한 부여

시스템 접속권한 책임자의 승인 전에는 권한부여가 되지 않도록 시스템을 조치하고, 불가피한 사후승인은 사유를 남기도록 개선하시기 바람