Security verification and auditing (PII)

(Smoke testS PRD)

Is the data filtered according to the application profile? Yes  No

If yes, indicate the types of filters applied:

|  |  |  |
| --- | --- | --- |
| **Filters** | **Applied / Not Applied** | **Observation** |
| Obfuscation | Yes    No |  |
| Anonimization | Yes    No |
| Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Yes    No |

Is the application access log logged? Yes  No

|  |
| --- |
| **Log Type** |

Is the rights exercised on users logged? Yes  No

|  |
| --- |
| **Rights log (example):** |

When replacing a backup, is it guaranteed that user data that is out of date, non-existent at the date is not restored? Yes  No

|  |
| --- |
| **How a backup is performed:** |

Before the attack (example: ransomware) are backups not affected? Yes  No

|  |
| --- |
| **Security of personal data backups:** |

Is there a DLP solution that monitors and controls access to personal data? Yes  No

|  |
| --- |
| **DLP solution (example):** |