Clean form

|  |
| --- |
| **1.** **DATA BREACH NOTIFICATION** |
| TYPE OF NOTIFICATION: |
| PRELIMINARY |
| COMPLETE |
| COMPLEMENTARY (FOLLOW-UP REPORT)  WHEN APPLICABLE, DATA ABOUT PRELIMINARY NOTIFICATION TO BE COMPLETED: ID OF PRELIMINARY NOTIFICATION: DATE: |

|  |
| --- |
| **2.** **DATA PROTECTION OFFICER IDENTIFICATION** |
| NAME: SURNAME: |
| ID NUMBER: PHONE NUMBER: EMAIL: |
| ADDRESS: ZIP CODE: |
| REGION: CITY: COUNTRY: |

|  |
| --- |
| **3.** **DATA CONTROLLER IDENTIFICATION** |
| NAME:  PUBLIC  PRIVATE |
| ID NUMBER: PHONE NUMBER: EMAIL: |
| ADDRESS: ZIP CODE: |
| REGION: CITY: COUNTRY: |

|  |  |
| --- | --- |
| **4.** **DATA PROCESSOR IDENTIFICATION** | |
| IS THERE ANOTHER ORGANISATION INVOLVED IN THIS DATA BREACH?  YES  NO | (TO BE FILLED WHEN APPLICABLE) |
| NAME:  PUBLIC  PRIVATE | |
| ID NUMBER: PHONE NUMBER: EMAIL: | |
| ADDRESS: ZIP CODE: | |
| REGION: CITY: COUNTRY: | |

|  |  |  |
| --- | --- | --- |
| **5.** **TIMELINE OF DATA BREACH** | | |
| DATA OF AWARENESS: | ACTUAL  ESTIMATED |  |
| MEANS OF DETECTION: | | |
| REASONS FOR LATE NOTIFICATION (72h AFTER DETECTION): | | |
| BEGINNING DATE: | ACTUAL  ESTIMATED | UNKNOWN |
| IS THE BREACH RESOLVED? | YES  NO |  |
| RESOLVED DATE: | ACTUAL  ESTIMATED | (IF NOT RESOLVED FILL WITH ESTIMATED DATE) |

|  |
| --- |
| **6.** **ABOUT THE DATA BREACH** |
| SUMMARY OF THE INCIDENT: |
| CONFIDENTIALITY (UNAUTHORIZED ACCESS / DISCLOSURE) TIPOLOGY : INTEGRITY (UNAUTHORIZED MODIFICATION)  AVAILABILITY (LOSS OR DESTRUCTION OF THE DATA) |



|  |
| --- |
| NATURE OF THE INCIDENT: |
| E-WASTE (PERSONAL DATA STILL PAPER LOST OR STOLEN OR LEFT INCORRECT DISPOSAL OF PRESENT ON OBSOLETE DEVICE) INSECURE LOCATION PERSONAL DATA ON PAPER  HACKING MALWARE (e.g. ransomware) PHISHING  MAIL LOST OR OPENED DEVICE LOST OR STOLEN UNINTENDED PUBLICATION  PERSONAL DATA DISPLAYED TO PERSONAL DATA SENT TO WRONG VERBAL UNAUTHORIZED WRONG RECIPIENT RECIPIENT DISCLOSURE OF PERSONAL  DATA  OTHER: |
| CAUSE: |
| INTERNAL (NON INTERNAL EXTERNAL (NON EXTERNAL MALICIOUS ACT) (MALICIOUS ACT) MALICIOUS ACT) (MALICIOUS ACT) |
| PREVENTATIVE MEASURES: |

|  |
| --- |
| **7.** **ABOUT THE BREACHED DATA** |
| REGULAR DATA: |
| BASIC PERSONAL IDENTIFIERS IDENTIFICATION DATA (USER, CONTACT DETAILS  PASSWORD)  NATIONAL ID NUMBERS ECONOMIC AND FINANCIAL DATA CRIMINAL CONVICTIONS LOCATION DATA PROFILE DATA  OTHER: |
| SPECIAL CATEGORY OF DATA: |
| RELIGIOUS OR PHILOSOPHICAL DATA REVEALING RACIAL OR POLITICAL OPINIONS BELIEFS ETHNIC ORIGIN  HEALTH DATA TRADE UNION MEMBERSHIP SEX LIFE DATA  GENETIC DATA BIOMETRIC DATA OTHER: |
| APPROXIMATE NUMBER OF PERSONAL DATA RECORDS CONCERNED : |



|  |
| --- |
| **8.** **ABOUT THE DATA SUBJECTS** |
| PROFILE OF THE DATA SUBJECT: |
| COSTUMERS USERS EMPLOYEES SUBSCRIBERS CHILDREN  STUDENTS PATIENTS OTHER: |
| APPROXIMATE NUMBER OF DATA SUBJECTS AFFECTED : |

|  |
| --- |
| **9.** **POTENTIAL CONSEQUENCES OF THE BREACH** |
| CONFIDENTIALITY BREACH: |
| LARGER DISTRIBUTION THAN NECESSARY DATA MAYBE EXPLOITED FOR OTHER PURPOSES  DATA MAY BE LINKED WITH OTHER INFORMATION OTHER: |
| INTEGRITY BREACH: |
| DATA MAY HAVE BEEN MODIFIED AN USED THOUGH IT IS NO LONGER VALID  DATA MODIFIED AND USED FOR OTHER PURPOSES OTHER: |
| AVAILABILITY BREACH : |
| LOSS OF THE ABILITY TO PROVIDE A CRITICAL SERVICE FOR THE AFFECTED DATA SUBJECTS  ALTERATION OF THE AVAILABILITY TO PROVIDE A CRITICAL SERVICE TO OTHER:  THE DATA SUBJECTS |
| NATURE OF THE POTENTIAL IMPACT FOR THE DATA SUBJECTS: |
| LOSS OF CONTROL OVER THEIR PERSONAL DATA FRAUD  IDENTITY THEFT DISCRIMINATION LIMITATION OF THEIR RIGHTS  DAMAGE TO REPUTATION FINANCIAL LOSS UNAUTH. PSEUDONYMISATION REVERSAL LOSS OF CONFIDENTIALITY OF PERSONAL DATA AFFECTED BY PROFESSIONAL SECRET  OTHER: |
| SEVERITY OF THE POTENTIAL IMPACT FOR THE DATA SUBJECTS |
| NEGLIGIBLE  LIMITED  SIGNIFICANT  MAXIMAL |
| MEASURES TAKEN BY THE CONTROLLER TO ADDRESS THE BREACH |

|  |
| --- |
| **10. COMMUNICATION TO DATA SUBJECTS** |
| INFORMATION OF DATA SUBJECTS |
| YES  NO BUT THEY WILL BE INFORMED  NO, THEY WILL NOT BE INFORMED  NOT YET DEFINED |
| WHEN APPLICABLE, DATE OF WHEN INFORMATION WAS GIVEN TO DATA SUBJECTS: |
| WHEN APPLICABLE, NUMBER OF DATA SUBJECTS INFORMED: |
| WHEN APPLICABLE, MEANS OF COMMUNICATION USED TO INFORM TO DATA SUBJECTS |
| WHEN APPLICABLE, REASON FOR NOT INFORMING DATA: |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **11. CROSS BORDER NOTIFICATIONS** | | | | | | | | |
| THERE ARE OTHER EU MEMBER STATES CONCERNED BY THE BREACH  INDICATE THE EU MEMBER STATES WITH DATA SUBJECTS AFFECTED BY THE DATA BREACH (A), AND IF OTHER DPAs HAVE BEEN NOTIFIED (N): | | | | | | | | |
| A | N |  | A | N |  | A | N |  |
|  |  | ALL MEMBER STATES |  |  | AUSTRIA |  |  | BELGIUM |
|  |  | BULGARIA |  |  | CROATIA |  |  | CYPRUS |
|  |  | CZECHIA |  |  | DENMARK |  |  | ESTONIA |
|  |  | FRANCE |  |  | FINLAND |  |  | GERMANY |
|  |  | GREECE |  |  | HUNGARY |  |  | IRELAND |
|  |  | ITALY |  |  | LATVIA |  |  | LITHUANIA |
|  |  | LUXEMBOURG |  |  | MALTA |  |  | NETHERLANDS |
|  |  | POLAND |  |  | PORTUGAL |  |  | ROMANIA |
|  |  | SLOVAKIA |  |  | SLOVENIA |  |  | SWEDEN |

|  |
| --- |
| **12. RELEVANT DOCUMENTS** |
| OTHER RELEVANT DOCUMENTS ATTACHED |

**Informative clause on data protection:**

Personal data will be processed by the Spanish Data Protection Authority and incorporated into the processing activity “Management of personal data breaches”, the purpose of which is the management and evaluation of the notification of personal data breaches.

Purpose based on compliance with legal obligations that the General Data Protection Regulation / General Telecommunications Law imposes on the Spanish Data Protection Authority.

Personal data may be communicated to the CERT (Computer Emergency Response Team) of the National Cryptologic Center (CCN), to the State Security Forces and Bodies, to the European Data Protection Committee, to the Data Protection Authorities of the European Union, and the network of computer security incident response teams ("CSIRT network"), created by Directive (EU) 2016/1148 on measures to ensure a high common level of security for networks and information systems in the Union.

The data will be kept for the time necessary to fulfill the purpose for which they have been collected and to determine the possible responsibilities that may arise from said purpose and the processing of the data. The regulations on archives and Spanish documentary heritage will apply.

You can exercise your rights of access, rectification, erasure and portability of your data, to restriction and object to its treatment, as well as not being the subject of automated individual decission-making, when appropriate, against the Spanish Data Protection Authority, C / Jorge Juan, 6, 28001- Madrid or at the email address [dpd@aepd.es](mailto:dpd@aepd.es)