DEMO
(40% of full document)

BREACH PROCEDURE

1. Any person who has contact with personal data should be aware of potential, most likely breaches of personal data protection characteristic of their area of activity. That person is obliged to notify their direct supervisor immediately of any potential breaches – a minimum solution is to make such persons acquainted with Appendix No. 9 adapted to the situation of a given undertaking.
2. In addition to using Appendix No. 9, at least once a year the scenarios included in Tables I–IV (General Risk Assessment), containing a list of exemplary scenarios of potential infringements, should be reviewed in the form of a discussion with all the persons authorised to process information or represent individual departments.
3. The discussion should be summed up in the form of minutes, which should account for the agreed conclusions in which new threat scenarios are accounted for or stating that there is no need for any modification of the currently examined threat scenarios.
4. Having become aware of a potential personal data breach, the circumstances of a reported incident must be examined immediately.
5. An examination of the incident circumstances must not be completed later than within 24 hours from the time of becoming aware of a potential breach.
6. In the event of incidents which require a longer analysis in order to confirm or exclude a breach, a written justification of a longer examination must be prepared.
7. Having examined the breach, the first part of a breach report, constituting Appendix 14a to the Security Policy, should be filled in with all the information required therein.
8. If it is confirmed that there was a personal data breach, the second part of the report, accounting for the steps specified in items 9–18, must be filled in immediately:

Resource value	**Information category**
(4) **Sensitive**	**Exclusively: data concerning health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for the purpose of identification), data concerning sex life or sexual orientation**
(3) **Financial**	**E.g. amount of salary, history of financial transactions, documents**

9. It should be determined which categories of personal data were affected by the breach by selecting one of the four categories included in the table below:

	related to the use of banking services, investments, credit cards, invoices, insurance documents relating to the financial situation
(2) **Behavioural** (pointing to certain behaviours)	**E.g. an ordinary Web browser history, information on location (e.g. navigation applications), web traffic information (billings, IP number), information on personal habits and routines**
(1) **Simple**	**E.g. name and surname, professional experience, qualifications, education, contact details (email, telephone number)**

10. A breach concerning data may fall into one of the following categories::
    - "**Simple**" breach is given **1 point**
    - "**Behavioural**" breach is given **2 points**
    - "**Financial**" breach is given **3 points**
    - "**Sensitive**" breach is given **4 points**

(Points for the data categories do not add up, the highest possible value should be adopted)

11. Context must be taken into account, which may make the result higher (e.g. from 1 to 4) or lower (e.g. from 4 to 1). Any time the basic result is modified, the reasons for a modification to the score must be clearly stated.

12. The breach elements which increase a basic result:

    - **the amount of data** concerning an individual person (whether it is a single document or a set of documents, whether it is information covering the last week or the last year)
    - **specific profile of activity** of the data subject concerned by the breach (whether the company is involved in a job placement programme for the unemployed or the disabled, or whether it provides medical services or services related to philosophical beliefs or sexual orientation, etc.)
    - **specific role or situation of the data subject(s)** concerned (e.g. a leak of private telephone numbers of people known to the general public, such as the players of a popular football team)

13. The breach elements which decrease a basic result:

    - **out-of-date status**, invalidity of the data, such as a mailing list based on which shipments could not be made effectively
    - **public availability** of the data if, before the breach, the data were in the public domain or easily accessible from publicly available sources
    - **nature of information,** if based on the context, it is obvious that the information cannot do any harm to the data subject(s)

    Example of a situation where the context does not increase the score:
    - a sheet of paper containing the names and surnames of the participants of a standard company training is blown out the window. The sheet contained "simple data" and the situation itself does not entail any additional circumstances.

    Example of a situation where the context does increase the score:
    - a sheet of paper containing names and surnames is blown out the window of an organisation involved in helping alcohol addicts. By establishing a connection between the names and surnames contained there with their source, it can be concluded that the scope of disclosed information includes alcohol addicts, addiction details, i.e. sensitive data – in this context the score should be increased from 1 to 4.

    Example of a situation where the context decreases the score:

The medical certificate of a John Smith indicating his perfect health is blown out the window. Formally this is a piece of information concerning a subject's medical condition, so the basic score should be 4; however, the context indicates that it is not going to affect the subject's situation in any negative way. The situation would be different if the certificate indicated a certain disease or even complaints.

14. Once the **information category (IC)** is established and the **context** is accounted for, it is necessary to take into account the elements which affect the **ease of identification (EI) (**this factor must be accounted for when calculating **Severity** solely in the case of confidentiality breaches; if only a breach of availability took place, the score specified in item 17 should be applied**)**:

a) **Name and surname** – score is assigned:
0.25 points – if the name and surname are included but, on a national scale, this is a very common name and surname (such as John Smith)
0.5 points – if the name and surname are included but, on a national scale, this surname is rather rare
0.75 points – if there are only a few people that have the same name and surname in a small town or just one person (and the incident can be linked to the place of residence)
1 point – if the date of birth and email are also included

b) **Identity card, passport, personal identity number**
0.25 points – if only a specific number has been disclosed in a given breach, and there is no link to the specific name, surname or other information which would enable identification
0.75 points – if the number includes the date of birth (as in the case of the Polish personal identification number) and is linked to other information, for example, address of residence or email
1 point – in the case of a scan of the identity card featuring the holder's photo

c) (…)