

Data Protection Impact Assessment (DPIA) Document



Plan of Action and Executive Summary

As the final step in conducting a DPIA (Data Protection Impact Assessment), an action plan must be developed describing all control measures defined to address the identified risks and concluding on the outcome obtained.

An action plan is the set of initiatives to be implemented in order to apply controls that help reduce the risk of a processing activity to an acceptable level.

The conclusion of the DPIA should be based on the level of residual risk obtained during the risk management phase, assessing whether it is high or considered acceptable and within reasonable limits.

Thus, after the risk assessment, it can be stated that the identified risks fall within acceptable levels, mainly due to the potential impact if the risk were to materialize. In view of this, the action plan to be adopted by THN consists of maintaining compliance with the technical and organizational security measures described and already implemented, in order to sustain the acceptable risk levels analyzed in this DPIA.

In any case, the following measures must be reviewed periodically:

1. Ensure that users affected by this system have been informed of the processing characteristics and that they are interacting with an AI system.
2. Verify that the AI system is, in all cases, subject to human oversight.
3. Implement an effective internal procedure for the retention and storage periods of chatcall data.
4. Ensure that the user has given their explicit consent to the processing.

If the measures outlined in this DPIA are abandoned or not followed, risk levels may increase, which would make it necessary to apply additional safeguards to reduce such risks and bring them back to acceptable levels.

Consequently, it has been determined that the processing activity can be carried out.