VANGUARD PROJECT- GDPR INFORMATION NOTICE

The principles of fair and transparent processing require the data subject be informed of the existence of the processing operation and its purposes. Complying with article 14 of the GDPR[1] and considering that the provision of such information proves impossible or would involve a disproportionate effort that would seriously impair the achievement of the objectives of the processing, the controller has taken the appropriate measures to protect the data subject's rights and freedoms and legitimate interests making the information about the processing publicly available. (article 14.5(b) GDPR)

The data controller

The data controller is ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L. (hereinafter "Atos"), established in this address: C/ Albarracín 25, 28037 Madrid, Spain.

Purpose of data processing and legal basis

The lawfulness base of processing is the legitimate interests of the data controller (article 6.1(f) GDPR). The processing is carried out to comply with Atos contractual obligations in the VANGUARD project where other organizations/companies are participating (consortium members). VANGUARD is a research and development project co-funded by the European Commission's Horizon Europe program, under grant agreement no. 101121282.

This privacy notice is specific and limited to the processing activities where Atos is in charge, according to the grant agreement, in relation to the VANGUARD project.

The purpose of data processing is to train two AI based tools. See more information below.

Legitimate interest pursued

The project

VANGUARD aims at strengthening the fight against trafficking in human beings (THB) by integrating advanced technological solutions, knowledge, awareness, and training, to disrupt the trafficking chain at an early stage and address the culture of impunity. In particular, VANGUARD seeks to provide better intelligence regarding THB with a specific focus on trafficking for sexual exploitation, labor exploitation, and forced criminality. This will be achieved by developing a modular and reliable set of tools to detect, identify, investigate, and prevent THB activities carried out online and at border checkpoints.

The purpose of the processing

Personal data will be used to train two AI based tools: (1) the first tool aims at detecting and tracking selected persons of interest across the public areas of airports; (2) the second tool aims at detecting tattoos and birthmarks in images and at finding specific tattoos and birthmarks in images kept in the project database.

[1] GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

These tools assist in the execution of the tasks explained above, but they do not make decisions. No automated decisions will be made. Decisions will always be made by individuals with the necessary competence and legal authorization.

It is important to highlight that under no circumstances can the data processing give rise to issues such as discrimination, identity theft or fraud, financial losses, damage to reputation, breaches of confidentiality of data subject to professional secrecy, or any other significant economic or social harm.

Personal data processed

The following publicly available datasets will be processed:

- BIVTatt-dataset [1]
  (https://github.com/mnicolas94/BIVTatt-Dataset)
  BIVTatt dataset contains cropped images of tattoos; full images of people do not appear.
- Human re-identification_recognition_Market1501 dataset [2]
  (https://paperswithcode.com/dataset/market-1501)
  Market-1501 is a large-scale public benchmark dataset for person re-identification. Data are anonymized before the processing.
- QMUL underground identification (GRID) dataset [3] [4] [5]
  (https://personal.ie.cuhk.edu.hk/~ccloy/downloads_qmul_underground_reid.html)
  GRID dataset contains images of pedestrian used for research and development of person re-identification algorithms in surveillance. Data are anonymized before the processing.

No special categories of personal data (art. 9(1) GDPR) are foreseen to be collected.

Minimization and proportionality measures to limit the processing of personal data as much as possible have been adopted: selection criteria have been established, and only relevant data have been processed.

Data transfers

The controller will not transfer personal data to any recipient. No international data transfers will be made.

The period for which the personal data will be stored

Data will be stored until the end of the project, foreseen in October 2026, plus 6 months to comply with legal and administrative obligations and procedures.

Security measures

Atos has implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Personal data are anonymized before being used to train the tools developed in the project and are protected with appropriate security measures. The main security measures included in Atos' corporate platform are listed next: (1) Advance Threat Protection: Antivirus, network inspection, firewall, tamper protection. (2) Network Access Control. (3) Cloud-based proxy, including URL filtering. (4) Disk encryption: Mandatory and automatic encryption after the Operating System installation, done

transparently (using TPM chip). (5) Two-Factor Authentication: For access to corporate web applications (SharePoint, Outlook, etc.), combined with a Single Sign-On portal. (6) Mail encryption. (7) Physical access security measures to access Atos buildings.

Data subject rights

The exercise of these rights recognized in GDPR, could be limited depending on the context of the processing activity and the request:

- Right of information: The right to receive information related to your personal data processed in a transparent and intelligible way.
- Right of access: The right to ask for a copy of your personal information.
- Right to rectification: The right to ask for a rectification of your personal data you think is inaccurate. Also, you have the right to ask for completion of information you think is incomplete.
- Right to erasure: The right to ask for the erasure of your personal information without undue delay, in certain circumstances.
- Right to restriction of processing: The right to ask for restriction of processing your personal data in certain circumstances.
- Right to object to processing: The right to object to the processing of your personal data in certain circumstances.
- Right to portability: The right to ask for the transfer of the personal information you gave to us to another organization in a structured, commonly used format.
- Right to lodge a complaint with the competent data protection authority. For the processing activities carried out, the competent authority is the Spanish Data Protection Agency (AEPD): https://www.aepd.es/

For the exercise of your rights, please contact dl-es-dpo-atos@atos.net

References

[1] Nicolás-Díaz, Miguel; Morales-González, Annette; and Méndez-Vázquez, Heydi (2019), Deep Generic Features for Tattoo Identification. Iberoamerican congress on pattern recognition, pages 272-282

[2] Liang Zheng*, Shengjin Wang, Liyue Shen*, Lu Tian*, Jiahao Bu, and Qi Tian. Person Re-identification Meets Image Search. Technical Report, 2015. (*equal contribution)

[3] C. Liu, S. Gong, and C. C. Loy. On-the-fly Feature Importance Mining for Person Re-Identification. Pattern Recognition, vol. 47, no. 4, pp. 1602-1615, 2014 (PR)

[4] S. Gong, M. Cristani, S. Yan, C. C. Loy (Eds.) Person Re-Identification. Springer, January 2014

[5] C. Liu, S. Gong, C. C. Loy, and X. Lin; In Gong, Cristani, Yan, Loy (Eds.) Evaluating Feature Importance for Re-Identification. Person Re-Identification, Springer, January 2014