# Offer #2022-05011

# PhD Position F/M Trustworthy multi-site privacy-preserving technologies

**Contract type :** Fixed-term contract

**Level of qualifications required :** Graduate degree or equivalent

**Fonction :** PhD Position

**Level of experience :** Up to 3 years

## About the research centre or Inria department

The Inria Lille - Nord Europe Research Centre was founded in 2008 and employs a staff of 360, including 300 scientists working in fifteen research teams. Recognised for its outstanding contribution to the socio-economic development of the Hauts-De-France région, the Inria Lille - Nord Europe Research Centre undertakes research in the field of computer science in collaboration with a range of academic, institutional and industrial partners.

The strategy of the Centre is to develop an internationally renowned centre of excellence with a significant impact on the City of Lille and its surrounding area. It works to achieve this by pursuing a range of ambitious research projects in such fields of computer science as the intelligence of data and adaptive software systems. Building on the synergies between research and industry, Inria is a major contributor to skills and technology transfer in the field of computer science.

## Context

This PhD student position will be supported by theHE Trumpet project.

While AI techniques are becoming ever more powerful, there is a growing concern about potential risks and abuses. As a result, there has been an increasing interest in research directions such as privacy-preserving machine learning, explainable machine learning, fairness and data protection legislation. Privacy-preserving machine learning aims at learning (and publishing or applying) a model from data while the data is not revealed. Notions such as (local) differential privacy and its generalizations allow to bound the amount of information revealed.

The overall goal of the TRUMPET project is to research and develop novel privacy enhancement methods for Federated Learning, and to deliver a highly scalable Federated AI service platform for researchers, that will enable AI-powered studies of siloed, multi-site, cross-domain, cross-border European datasets with privacy guarantees that exceed the requirements of GDPR.

INRIA's MAGNET team will contribute among others to tasks involving AI algorithms and architectures, federated Learning, privacy platforms, privacy measurement and metrics, privacy-enhancing technologies and applied cryptography

## Assignment

The recruited PhD student will collaborate with colleagues in the MAGNET team and the TRUMPET project consortium in general.  Part of the work may involve travel to other partners.

If the research features a prototype, it will contribute to the project's open source library and may be supported by engineers in the team.

Possible topics of research include (but are not limited to):

- Cryptography-based strategies to improve the security of privacy-preserving AI systems.
- Inference methods for privacy assessment
- Design and development of the TRUMPET platform and its supporting algorithms

## Main activities

- Contribute to the research of the TRUMPET project

- Collaborate with other MAGNET and TRUMPET team members
- Disseminate research results

## Skills

The ideal candidate will have the following skills:

- Good mastery of English
- A strong background in computer science and mathematics.  Subject matters which will be needed during the research include (but are not limited to) machine learning, statistics, cryptography, distributed systems, constraint programming.
- Good programming skills (e.g., C/C++ or python) and supporting tools.
- Relational skills, e.g., working in a team, effective reporting and communication with all involved stakeholders.

## Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

## Remuneration

1st and 2nd year : 2051 € gross monthly salary (before taxes)

3rd year : 2158 € gross monthly salary (before taxes)

## General Information

- **Theme/Domain :** Data and Knowledge Representation and Processing
  Statistics (Big data) (BAP E)
- **Town/city :** Villeneuve d'Ascq
- **Inria Center :** Centre Inria de l'Université de Lille
- **Starting date :** 2023-09-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2023-09-30

## Contacts

- **Inria Team :** MAGNET
- **PhD Supervisor :**
  Ramon Jan / jan.ramon@inria.fr

## About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

## The keys to success

We are looking for a candidate with a strong background in computer science, with interest in research (including the mathematics needed to realize privacy) who welcomes the broad range of challenges leading to a successful result.

Candidates should provide sufficient information to support their application, the page https://team.inria.fr/magnet/how-to-apply/ lists the minimum information desired (which is more than what is stricly required by the online submission platform).

**Warning** : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

## Instruction to apply

CV + application letter + recommendation letters + List of publications

Academic transcripts, thesis, project report

**Defence Security :**
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

**Recruitment Policy :**
As part of its diversity policy, all Inria positions are accessible to people with disabilities.