université PARIS-SACLAY

INSTITUTE DATAIA
Data Science, Intelligence & Society

D2C
DATAIA CLUB CONNECTION

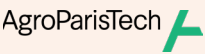
CYBERSECURITY & AI


université
PARIS-SACLAY

université
évry
val-d'essonne
université
PARIS-SACLAY

UVSQ
université PARIS-SACLAY

CentraleSupélec

école
normale
supérieure
paris—saclay

AgroParisTech

cea

INRAE

Inria

cnrs

ONERA
THE FRENCH AEROSPACE LAB

FM
JH
FONDATION MATHÉMATIQUE
JACQUES HADAMARD

CentraleSupélec
EXED

GUSTAVE
ROUSSY
CANCER CAMPUS
GRAND PARIS

Institut Mines-Télécom
Business School

INSTITUT
d'OPTIQUE
GRADUATE SCHOOL
ParisTech

IHES

DATAIA PARIS-SACLAY INSTITUTE

Located within the **Paris-Saclay University** (12th Shanghai ranking), it is the **first French ecosystem in Data Sciences, AI and their societal impacts.**

MISSION

To bring together **multidisciplinary expertise and boost the collective strength of its partners** in the Paris-Saclay cluster with the aim of combining big data and AI technologies with social sciences and humanities for an AI at the service of humans.

IN FIGURES

14 DATAIA members

47 laboratories partners

800 full-time researchers

10 IA chairs out of 40 national

30 IA theses

450 PhD students per year

PAI
Programme d'Affiliation Industrielle

The Industrial Affiliation Plan (PAI) aims to boost the collective strength of the Institute's academic ecosystem and its industrial members. The services offered in response to the respective needs expressed include:

- Joint actions to support research;
- Sharing of experiences and collective needs;
- Facilitated access to recruitment;
- Access to training, seminars, workshops, etc.;
- Implementation of dedicated events (hackathons, challenges, etc.);
- Access to working places to increase exchanges.

D2C
DATAIA CLUB CONNECTION

The D2C system aims **upstream**, to present the priority research issues and to match them with the problems of industry. **Downstream**, to monitor contacts and opportunities for collaboration identified until they are set up and launched. It is part of the ambition to facilitate the establishment of several levels of collaboration and create a constructive dynamic:

1. Expertise / Student projects / Internships
2. Research collaborations / CIFRE theses
3. Joint laboratories / Joint teams
4. Multi-partner chairs

OBJECTIVES & PROGRAM

The main objectives of this D2C are focusing on :

- **Data Protection and AI Privacy**: Solutions for Secure AI Implementation
- **Secure Collaboration in Machine Learning, Models Protections**: Solutions for models protections and data used in a collaborative framework or in an environment with an assumed insufficient security level (zero trust)
- **Secure Chatbot and LLM Filtering**: Ensuring data and model confidentiality when used by third parties
- **Synthetic Data / Anonymization**: Anonymization of data used training models

DATAIA RESEARCHERS

Use of LLM to Anonymize a Text Maintening its Usefulness Design of Validation Techniques for Inference Attacks

Nicolas Anciaux (Inria Saclay)
Deputy Scientific Delegate Inria Saclay
Researcher of Petscraft Team

Human Detection, Measures and Improvement Platform Reality Check

Enguerand Chary (ENS Paris-Saclay, Centre Borelli)
Research Engineer

Cyber: from Components to Business Applications Data Sharing in a Decentralized Security Space

Jean-Michel Côme-Corneille (CEA List)
Head of Industrial Partnerships

Connection with Local and Global Differential Privacy

Pablo Piantadina - Director and Professor
Ulrich Aivodji - Associate Professor

DATAIA CLUB PAI PARTNERS

SERVIER
moved by you

Strengthen Data Protection in non-European Clouds? Facilitate Large-Scale Data Anonymization/Pseudonymiation

Stéphane Tournadre - Chief Information Security Officer

System X
INSTITUT DE RECHERCHE TECHNOLOGIQUE

Interface between AI and Cyber Training AI Models on Confidential Data Anomalies Detection

Reda Yaich - Senior Researcher, Head of Digital Security and Networks

PARTNERS & GUEST COMPANIES

Sefira AI

Building an AI Agent that Operates on a Sensitive Perimeter

Romain Laurent - CEO
Vincent Yuan - CTO

SKYLD

Protection of Models with the Risks of Reverse Engineering

Marie Paindavoine - CEO

OCTOPIZE
MIMETHIK DATA

Data Anonymisation through the Creation of Anonymous Synthetic Data

Olivier Breillacq - Researcher & R&D PM
Antoine Bachelier - Business Manager

INSTITUTIONAL PARTNERS

CONTACT

Eric TORDJEMAN
Head of Industrial Partnerships @DATAIA
eric.tordjeman@universite-paris-saclay.fr
eric-tordjeman

To learn more about DATAIA's Institute Industrial Affiliation Program :

université PARIS-SACLAY

INSTITUT DATAIA
Science des données, Intelligence & Société

DATAIA Paris-Saclay Institute
Université Paris-Saclay - Campus CentraleSupélec
3 rue Joliot Curie
91190 Gif-sur-Yvette

Communication Department
com-dataia@inria.fr

www.dataia.eu
@institut-dataia