



**CISPA**  
HELMHOLTZ CENTER FOR  
INFORMATION SECURITY

## Open Ph.D. and Postdoc Positions in Trustworthy AI and Reliable Machine Learning

The group of Krikamol Muandet (<http://www.krikamol.org/>) at CISPA Helmholtz Center for Information Security (<https://cispa.de/en>) in Saarbrücken, Germany has multiple openings for Ph.D. students and postdoctoral researchers with a strong interest in the broad areas of machine learning (ML). The group's research aims at understanding the principles that enable autonomous agents to learn from past experience and interact successfully with complex environments, and to use this understanding to design new learning algorithms. The research theme spans the following areas:

- **Prediction:** How do we design ML algorithms that can cope with distributional shifts? The topics of interest are domain adaption (DA), domain generalization (DG), out-of-distribution (OOD) generalization, and robustness. Kernel methods, kernel mean embedding of distributions, and applications thereof are our mathematical arsenal to tackle these problems.
- **Causation:** How do we leverage cause-effect relationships in improving ML models, and conversely how do we use sophisticated ML methods to aid causal inference in complex environments? Topics of interest are observational studies, unobserved confounders in causal inference, spurious correlation in machine learning, distributional treatment effects, counterfactual inference, and algorithmic decision making. Natural experiments and quasi-experimental designs such as instrumental variable (IV), proxy variables, and regression discontinuity design (RDD) offers tools to address these problems.
- **Regulation:** How do we regulate the deployment of ML models in heterogeneous environments to ensure the democratic use of AI? Topics of interest are feedback loops and strategic behaviour. To gain a better understanding of these problems, we will be adopting techniques from algorithmic game theory, mechanism design, social choice theory and other related sub-fields of economics.

The successful candidates are expected to pursue one of these research directions.

### What we look for

The candidates for the PhD positions are expected to have an excellent master's degree in Computer Science, Mathematics, Statistics, or a related discipline. A prior research experience and proficiency with programming languages are a plus. The candidates for postdoctoral researchers are expected to have an excellent PhD degree in Computer Science, Mathematics, Statistics, Economics, or a related discipline with a strong record of publications in top-tier venues such as ICML, NeurIPS, UAI, KDD, EC, AAMAS, AAI, FAccT, ICLR, AISTATS, JMLR, TPAMI, etc. Postdoc candidates with an Economics background are strongly encouraged to apply.

## **What we offer**

PhD students are full-time employees and are paid and receive benefits according to the E13 scale of the collective salary agreement for civil servants of the federal state (TVöD-Bund). The gross monthly salary, based on 39 hours per week and dependent on relevant experience usually ranges from ~4000€ to ~5000€. Additional benefits include roughly 6 weeks of paid annual leave; a collectively agreed annual special payment; paid sick leave; as well as maternity and parental leave; a complete educational program for PhD students including courses on science communication, time management and leadership; the possibility to set up a workplace at home in Germany; a pension scheme; the possibility to follow courses to learn German. Postdocs receive similar benefits as above. Salary classification is based on relevant experience periods. The research group has an annual budget for the members to purchase necessary research equipment and to attend international conferences.

The candidates will have the opportunity to collaborate with other research groups at CISPA (<https://cispa.de/en/research>) and with partners within the Helmholtz AI Cooperation Unit (<https://www.helmholtz.ai/>). We strongly encourage collaborations with neighboring research institutes at the Saarland Informatics Campus (<https://saarland-informatics-campus.de/en/>) such as Saarland University (UdS), Max Planck Institute for Informatics (MPI-INF), Max Planck Institute for Software Systems (MPI-SWS), Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI), as well as the Max Planck Institute for Intelligent Systems (MPI-IS) in Tübingen. International collaborations will be highly appreciated.

## **About CISPA**

The CISPA Helmholtz Center for Information Security provides a unique work environment that offers the advantages of a university department and a research laboratory alike. As the latest member of the Helmholtz Association, the largest research organization in Germany, CISPA has embarked on a mission: to rethink the digitalized world of the future from the ground up and make it safer through innovative cutting-edge research. In the medium term, the center will grow to more than 800 employees with not less than 60 Faculty and research group leaders. Faculty receive extremely competitive institutional funding, enjoy academic freedom, and build and lead their team of young researchers, and are granted the opportunity to teach graduate and undergraduate courses.

CISPA is located in Saarbrücken, in the tri-border area of Germany, France, and Luxembourg. We maintain an international and diverse work environment and seek applications from outstanding researchers worldwide. The working language is English. A command of German is not required for a successful career at CISPA.

## **How to apply**

The candidates should apply directly at <https://jobs.cispa.saarland/jobs>. In your cover letter, please include a brief explanation of why you are interested in working with me and which research directions you are most excited about. The latter may be explained in more detail in your research statement if you plan to submit one. The screening process will begin in October 2022 and continue until the positions are filled. Inquiries about the positions are welcome.