CODE OF ETHICS
Swiss Informatics Society SI

Document overview

Code of Ethics – English version

Code of Ethics – Enforcement procedures

Ethikrichtlinien – Leitsätze in Deutsch

Codex éthique – Les principes en français – en traduction!

Code of Ethics – Preamble, history & useful references.

Code of Ethics – Vorwort, Entstehung & weiterführende Referenzen

January 2019
SIG I&G

CODE OF ETHICS
Swiss Informatics Society SI

An adaptation of the 2018 ACM Ethics Code

---

1 General Ethical Principles

A computing professional in computing should…

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority.

Computing professionals should consider whether the results of their efforts will respect diversity, will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work that benefits the public good.

In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals are encouraged to promote environmental sustainability both locally and globally.

1.2 Avoid harm.

In this document, "harm" means negative consequences, especially when those consequences are significant and unjust. Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive.

Well-intended actions, including those that accomplish assigned duties, may lead to harm. When that harm is unintended, those responsible are obliged to undo or mitigate the harm as much as possible. Avoiding harm begins with careful consideration of potential impacts on all those affected by decisions. When harm is an intentional part of the system, those responsible are obligated to ensure that the harm is ethically justified. In either case, ensure that all harm is minimized.

To minimize the possibility of indirectly or unintentionally harming others, computing professionals should follow generally accepted best practices unless there is a compelling ethical reason to do otherwise. Additionally, the consequences of data aggregation and emergent properties of systems should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.

A computing professional has an additional obligation to report any signs of system risks that might result in harm. If leaders do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, a computing professional should carefully assess relevant aspects of the situation.

1.3 Be honest and trustworthy.

Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.

Computing professionals should be honest about their qualifications, and about any limitations in their competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to either real or perceived conflicts of interest or otherwise tend to undermine the independence of their judgment. Furthermore, commitments should be honored.

Computing professionals should not misrepresent an organization's policies or procedures, and should not speak on behalf of an organization unless authorized to do so.

1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and justice govern this principle. Fairness requires that even careful decision processes provide some avenue for redress of grievances.

Computing professionals should foster fair participation of all people, including those of underrepresented groups. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, nationality, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of the Code. Harassment, including sexual harassment, bullying, and other abuses of power and authority, is a form of discrimination that, amongst other harms, limits fair access to the virtual and physical spaces where such harassment takes place.

The use of information and technology may cause new, or enhance existing, inequities. Technologies and practices should be as inclusive and accessible as possible and computing professionals should take action to avoid creating systems or technologies that disenfranchise or oppress people. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.

1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

Developing new ideas, inventions, creative works, and computing artifacts creates value for society, and those who expend this effort should expect to gain value from their work. Computing professionals should therefore credit the creators of ideas, inventions, work, and artifacts, and respect copyrights, patents, trade secrets, license agreements, and other methods of protecting authors' works.

Both custom and the law recognize that some exceptions to a creator's control of a work are necessary for the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works. Computing professionals should not claim private ownership of work that they or others have shared as public resources.

1.6 Respect privacy.

The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.

Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should help to establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections.

1.7 Honor confidentiality.

Computing professionals are often entrusted with confidential information such as trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly articles, and patent applications. Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities. A computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

2 Professional Responsibilities

A computing professional in computing should…

2.1 Strive to achieve high quality in both the processes and products of professional work.

Computing professionals should insist on and support high quality work from themselves and from colleagues. Computing professionals should respect the right of those involved to transparent communication about the project. Professionals should be cognizant of any serious negative consequences affecting any stakeholder that may result from poor quality work and should resist inducements to neglect this responsibility.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

High quality computing depends on individuals and teams who take personal and group responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and with awareness of the social context in which their work may be deployed. Professional competence also requires skill in communication, in reflective analysis, and in recognizing and navigating ethical challenges. Upgrading skills should be an ongoing process and might include independent study, attending conferences or seminars, and other informal or formal education. Professional organizations and employers should encourage and facilitate these activities.

2.3 Know and respect existing rules pertaining to professional work.

"Rules" here include local, regional, national, and international laws and regulations, as well as any policies and procedures of the organizations to which the professional belongs. Computing professionals must abide by these rules unless there is a compelling ethical justification to do otherwise. Rules that are judged unethical should be challenged. A rule may be unethical when it has an inadequate moral basis or causes recognizable

harm. A computing professional should consider challenging the rule through existing channels before violating the rule. A computing professional who decides to violate a rule because it is unethical, or for any other reason, must consider potential consequences and accept responsibility for that action.

2.4 Accept and provide appropriate professional review.

High quality professional work in computing depends on professional review at all stages. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical reviews of others' work.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computing professionals are in a position of trust, and therefore have a special responsibility to provide objective, credible evaluations of computer systems and testimony to employers, employees, clients, users, and the public. Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Extraordinary care should be taken to identify and mitigate potential risks in machine learning systems. A system for which future risks cannot be reliably predicted requires frequent reassessment of risk as the system evolves in use, or it should not be deployed. Any issues that might result in major risk must be reported to appropriate parties.

2.6 Perform work only in areas of competence.

A computing professional is responsible for evaluating potential work assignments. This includes evaluating the work's feasibility and advisability, and making a judgment about whether the work assignment is within the professional's areas of competence. If at any time before or during the work assignment the professional identifies a lack of a necessary expertise, they must disclose this to the employer or client. The client or employer may decide to pursue the assignment with the professional after additional time to acquire the necessary competencies, to pursue the assignment with someone else who has the required expertise, or to forgo the assignment. A computing professional's ethical judgment should be the final guide in deciding whether to work on the assignment.

2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.

As appropriate to the context and one's abilities, computing professionals should share technical knowledge with the public, foster awareness of computing, and encourage understanding of computing. These communications with the public should be clear, respectful, and welcoming. Important issues include the impacts of computer systems, their limitations, their vulnerabilities, and the opportunities that they present. Additionally, a computing professional should respectfully address inaccurate or misleading information related to computing.

2.8 Access computing and communication resources only when authorized or when compelled by the public good.

Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code. A system being publicly accessible is not sufficient grounds on its own to imply authorization.

2.9 Design and implement systems that are robustly and usably secure.

Breaches of computer security cause harm. Robust security should be an essential consideration when designing and implementing systems. Computing professionals should perform due diligence to ensure the system functions as intended, and take appropriate

action to secure resources against accidental and intentional misuse, modification, and denial of service. As threats can arise and change after a system is deployed, computing professionals should integrate mitigation techniques and policies, such as monitoring, patching, and vulnerability reporting. Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner, providing appropriate guidance and remediation.

Computing professionals should discourage security precautions that are too confusing, are situationally inappropriate, or otherwise inhibit legitimate use.

In cases where misuse or harm are predictable or unavoidable, the best option may be to not implement the system.

3 Professional Leadership Principles

Leadership may either be a formal designation or arise informally from influence over others. In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. While these principles apply to all computing professionals, leaders bear a heightened responsibility to uphold and promote them, both within and through their organizations.

A computing professional in computing should…

3.1 Ensure that the public good is the central concern during all professional computing work.

People—including users, customers, colleagues, and others affected directly or indirectly—should always be a concern in computing. The public good should always be an explicit consideration when evaluating tasks associated with research, requirements analysis, design, implementation, testing, validation, deployment, maintenance, retirement, and disposal. Computing professionals should keep this focus no matter which methodologies or techniques they use in their practice.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.

Technical organizations and groups affect broader society, and their leaders should accept the associated responsibilities. Organizations—through procedures and attitudes oriented toward quality, transparency, and the welfare of society —reduce harm to the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation of computing professionals in meeting relevant social responsibilities and discourage tendencies to do otherwise.

3.3 Manage personnel and resources to enhance the quality of working life.

Leaders should consider the personal and professional development, accessibility requirements, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be used in the workplace.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.

Leaders should pursue clearly defined organizational policies that are consistent with the Code and effectively communicate them to relevant stakeholders. In addition, leaders should encourage and reward compliance with those policies, and take appropriate action when policies are violated. Designing or implementing processes that deliberately or negligently violate, or tend to enable the violation of, the Code's principles is ethically unacceptable.

3.5 Create opportunities for members of the organization or group to grow as professionals.

Educational opportunities are essential for all organization and group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties. These opportunities should include experiences that familiarize computing professionals with the consequences and limitations of particular types of systems.

3.6 Use care when modifying or retiring systems.

Interface changes, the removal of features, and even software updates have an impact on the productivity of users and the quality of their work. Leaders should take care when changing or discontinuing support for system features on which people still depend. Leaders should thoroughly investigate viable alternatives to removing support for a legacy system. If these alternatives are unacceptably risky or impractical, the developer should assist stakeholders' graceful migration from the system to an alternative. Users should be notified of the risks of continued use of the unsupported system long before support ends.

3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

Even the simplest computer systems have the potential to impact all aspects of society when integrated with everyday activities such as commerce, travel, government, healthcare, and education. When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems. Part of that stewardship requires establishing policies for fair system access, including for those who may have been excluded. That stewardship also requires that computing professionals monitor the level of integration of their systems into the infrastructure of society. As the level of adoption changes, the ethical responsibilities of the organization or group are likely to change as well. Continual monitoring of how society is using a system will allow the organization or group to remain consistent with their ethical obligations outlined in the Code. When appropriate standards of care do not exist, computing professionals have a duty to ensure they are developed.

4 Compliance with the Code

A computing professional in computing should…

4.1 Uphold, promote, and respect the principles of the Code.

The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles of the Code and contribute to improving them. Computing professionals who recognize breaches of the Code should take actions to resolve the ethical issues they recognize, including, when reasonable, expressing their concern to the person or persons thought to be violating the Code.

4.2 Treat violations of the Code as inconsistent with membership in the SI.

Each SI member should encourage and support adherence by all computing professionals regardless of SI membership. SI members who recognize a breach of the Code should consider reporting the violation to the SI, which may result in remedial action as specified in the SI 's Code of Ethics and Professional Conduct Enforcement Policy.

January 2019
SIG I&G

SI ETHICS CODE ENFOREMENT PROCEDURE

Schweizer Informatik Gesellschaft SI

Table of Content

SI Ethics Code Enforcement Procedures

The Swiss Informatics Society ("SI") expects all SI members and members of SI Special Interest Groups ("SIGs") (referred to in this Policy, together with SI members, as "Members") and assigned organizations ("AOs") to make a commitment to engage in ethical professional conduct and abide by SI's Ethics Code (the "Code").

The following bodies are involved in this procedure:

- SI General Assembly elects five to seven members of Ethic Committee ("EC") for the period of two years. The EC constitutes itself.
- SI Board processes appeals.

A. Complaint Resolution Procedure

Every Member may submit complaints to the EC concerning suspected violations of the Code by another Member. Any complaint should identify the Code provision(s) that were allegedly violated and describe in as much detail as possible the factual basis and list witnesses of the violation (if any). A complaint must be submitted within 60 days after the alleged violation is detected and within 3 years after violation. The privileges for the defendant of a complaint that are described in this policy only apply when the defendant of the complaint is a Member at the time of submission.

1. Initial Review

The EC will review the complaint within 30 days after submission. The EC may determine that a complaint is outside the scope of this Policy. A complaint will not be pursued if:

(i) it lacks sufficient factual allegations to investigate the complaint, or
(ii) the EC has good reason to believe it was made in bad faith, or

(iii) it is a subject of any legal action or governmental investigation.

The EC will notify the complainant of the decision to not process the complaint.

If the EC decides that further action under this Policy is appropriate, than

- if some facts are missing or not evident, EC asks the complainant for further documents and facts, which has to be submitted within 30 days
- provided EC has all needed information available, it informs the defendant about the complaint and asks for comment, which has to be submitted within 60 days.

2. Evaluation of Defendant Comments

EC evaluates the comment by the defendant and decides to reject or endorse the complaint within 30 days.

If EC decides based on the comment to reject the complaint then it informs both, the complainant and defendant about the rejection.
If EC decides to endorse the complaint, then it defines also the sanctions and informs both parties about the endorsement and sanctions.

Both parties can accept or reject the decision. If both parties accept the decision, the case is closed and the SI board is informed.

3. Mediation

Both parties have the right to challenge the EC decision by submitting an objection within 30 days after the decision has been issued.
EC provides the submitted objection including any attached evidence to the other party and organises within 60 days a hearing where both parties and witnesses are invited.
It's recommended that the lead of mediation is by an EC member not involved before in this case.

4 Decision after Mediation

Following the Mediation, the EC reviews the acquired facts and decides within 30 days whether the complaint violates SI's Ethics Code. Following determinations can result:

1 EC determines that it is more likely than not that the alleged Code violation(s) did not occur. EC informs involved parties about the rejection.

2 EC determines that indeed a Code violation occurred. In this case EC also defines what remedial sanction is appropriate. Without limitation, possible remediation may include issuance of a letter of admonishment which is not published, or one of the following sanctions published including the defendant's name
   - the defendant being barred from attendance at conferences for a specified time,
   - the defendant being barred from volunteering for SI activities for a specified time,
   - the defendant suspended from SI for a specified time,
   - the defendant is prohibited to publish in SI publications, or
   - expulsion of the defendant from SI and it's SIGs and AOs.

5. Appeal

Both parties have the right to challenge the decision based on mediation and appeal within 30 days after the decision has been issued. The appeal must be submitted in writing to the SI Board. SI Board requests all material pertaining to the case by EC.
SI Board takes a final decision and informs the appealing person and EC within 60 days.

B. Documentation of procedure execution

Minutes of the meetings will record the motions and actions taken but will not record the names of the complainant and witnesses. Each record relevant to the proceeding, including the complaint, comments, replies, materials, appeals and decisions submitted by the parties or collected by the EC will be retained for ten years by SI office.

C. Conflicts of Interest

No member of EC may participate in resolving a complaint if they have a conflict of interest. Conflicts of interest may include, but are not necessarily limited to,

- a personal or financial relationship with the complainant or defendant,
- a personal or financial interest in the outcome of the complaint or
- a personal involvement in or knowledge of the conduct at issue in the complaint.

A member of EC who believes he or she has a conflict of interest should promptly recuse him- or herself and disclose the nature of the conflict of interest to the EC Chair.

D. Confidentiality

During “Initial Review” all information about the case is restricted to EC and the complainant; the same if the “Initial Review” results in complaint rejection.

Until a final decision has been made, information is restricted to EC, complainant, defendant and witnesses, if any. In case the EC decision is appealed to the board, the board will be informed too.

Publications never include names of complainant and witnesses.

E. Policy Applicability

If at any point the EC determines that an authority is already involved in this complaint, then it suspends the procedure.
After the investigation of the appropriate authorities is completed, whether or not such involvement results in any criminal or civil sanctions, a complainant may request that EC continue its consideration of the complaint under this Policy, or EC may choose to do so without prompting.

F. No Retaliation

It is inconsistent with the Code to make threats or engage in acts of retaliation against individuals who in good faith report suspected violations of the Code. A Member who believes that he or she has been retaliated against for making a good-faith complaint under this Policy may use the above procedures to report the pertinent facts to the EC, who will consider the report as a complaint made under this Policy.

G. Costs

The complaint processing is up to the appeal for free.
An appeal is processed as soon as the appellant has paid a fee of CHF 100.- to SI office within 30 days.
There is no compensation for the plaintiff or defendant. Third parties can be paid expenses incurred from hearings out of SI’s funds.

SI Ethics Code

Anhang: Deutsche Übersetzung der Leitsätze

1. Allgemeine ethische Grundsätze
General Ethical Principles

Eine Informatikerin soll ...
(A computing professional in computing should…)

1.1 sich der gesellschaftlichen Verantwortung bewusst sein
(Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.)

1.2 Schaden zu vermeiden trachten
(Avoid harm.)

1.3 ehrlich und vertrauenswürdig sein
(Be honest and trustworthy.)

1.4 fair sein und Diskriminierung vermeiden
(Be fair and take action not to discriminate.)

1.5 die Arbeiten anderer achten
(Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.)

1.6 die Privatsphäre anderer respektieren
(Respect privacy.)

1.7 deklarierte Vertraulichkeit beachten
(Honor confidentiality.)

2. Berufliche Verantwortung
(Professional Responsibilities.)

Ein Informatiker soll ...
(A computing professional in computing should…)

2.1 nach hoher Qualität der Arbeitsprozesse und der Produkte streben
(Strive to achieve high quality in both the processes and products of professional work.)

2.2 hohe Standards bzgl. beruflicher Kompetenz, des Verhaltens und der ethischen Praxis aufrechterhalten
(Maintain high standards of professional competence, conduct, and ethical practice.)

2.3 existierende Regeln fachlicher Arbeit kennen und befolgen
(Know and respect existing rules pertaining to professional work.)

2.4 angemessenes professionelles Feedback akzeptieren und leisten
(Accept and provide appropriate professional review.)

2.5 umfassende und gründliche Evaluation von IT-Systemen und ihren Folgen, inkl. Analyse der Risiken leisten
(Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.)

2.6 nur in den Gebieten der fachlichen Kompetenz Arbeit leisten
(Perform work only in areas of competence.)

2.7 öffentliches Bewusstsein und Verständnis von Informations- und verwandten Technologien und ihren Auswirkungen fördern
(Foster public awareness and understanding of computing, related technologies, and their consequences.)

2.8 auf IT und Kommunikationsressourcen nur bei entsprechender Autorisierung zugreifen oder wenn öffentliches Interesse überwiegt
(Access computing and communication resources only when authorized or when compelled by the public good.)

2.9 Entwurf und Implementierung von Systemen sicher gestalten
(Design and implement systems that are robustly and usably secure.)

3. Grundsätze in Führungspositionen und Vorbildfunktionen
(Professional leadership principles.)

Eine Informatikerin soll ...
(A computing professional in computing should…)

3.1 in der beruflichen Tätigkeit stets das öffentliche Wohl beachten
(Ensure that the public good is the central concern during all professional computing work.)

3.2 soziale Verantwortung der Mitglieder der Gruppe oder Organisation ansprechen, dazu ermuntern und sie bewerten
(Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.)

3.3 Mitarbeiter und Ressourcen zur Verbesserung des Arbeitslebens anleiten und einsetzen
(Manage personnel and resources to enhance the quality of working life.)

3.4 Strategien und Prozesse, die die Prinzipien dieser Ethikrichtlinien widerspiegeln, formulieren, anwenden und unterstützen
(Articulate, apply, and support policies and processes that reflect the principles of the Code.)

3.5 Gelegenheiten zur beruflichen Weiterentwicklung für Mitglieder der Gruppe oder Organisation schaffen
(Create opportunities for members of the organization or group to grow as professionals.)

3.6 bei der Änderung oder Stilllegung von Systemen sorgfältig sein
(Use care when modifying or retiring systems.)

3.7 Systeme, die Teil der gesellschaftlichen Infrastruktur werden, erkennen und mit besonderer Sorgfalt behandeln
(Recognize and take special care of systems that become integrated into the infrastructure of society.)

4. Einhalten der Ethikrichtlinien
(Compliance with the code.)

Ein Informatiker soll ...
(A computing professional in computing should…)

4.1 diese Ethikrichtlinien verbreiten und befolgen
(Uphold, promote, and respect the principles of the Code.)

4.2 Verstösse gegen diese Ethikrichtlinien als unvereinbar mit der SI-Mitgliedschaft behandeln
(Treat violations of the Code as inconsistent with membership in the ACM.)

CODE OF ETHICS
Swiss Informatics Society SI

Preamble – January 2019

The SI special interest group on IT & Society has drafted an update of the SI Ethics code and plans to submit it to the next general assembly for approval.

Why do we need an ethics code? Most professional societies have some kind of ethics code (it might be named differently in other professions, though). Such guidelines help professionals to decide in ethical conflict situations. For example, is it ethically responsible for a computer scientist to work in a project that aims to optimize drone warfare? Questions like these are all but theoretical – many of our colleagues in the US have faced similar questions in the recent past (see the links at the end of this document).

Ethics codes are no binary algorithm that output true or false when fed with an ethical problem. Instead, ethics codes provide guidelines based on general and professional values that help professionals to come to an ethical decision. This also means that, based on the same guidelines, different persons can come to different conclusions in seemingly the same situation.

Why is an update of the SI ethics code necessary *now*? The currently existing ethics guidelines have been approved by the general assembly in 2005. This was even before the invention of the iPhone! This is, since the last update IT has become an even more fundamental technology in society and business, and our work has an even bigger impact on everybody‘s life. This implies a larger responsibility of computer scientist to implement digitalization in a non-disruptive way.

All in all, the new guidelines are very similar to the old ones. Changes have been necessary mainly in order to provide guidance how to deal with the disruptive aspects of digitalization (such as discrimination, privacy threats).

Why have we adopted the ethics code of ACM? Like for the eixsting one, we have adopted ACM‘s ethics code also for the updated ones for several reasons. We are convinced that it is adquate and comprehensive, and in particular appreciate the principles dealing with new developments (e.g., social networks). Furthermore, the update of the code was very thoroughly discussed. Finally, adopting ACM‘s code shows our connection to the international community of computer scientists and IT societies.

The structure of the ethics code has not changed significantly. It consists of four parts:

1 general principles regarding the role of computer scientists in the society;

2 principles of computer science professionals;

3 leadership principles for professionals that additionally are managers, teachers, topic experts, etc;

4 The enforcement of the code.

The current code has a fifth section which deals with the role of SI. This part has been omitted in the update.

We hope that SI members will live the code, in that it provides support and guidance to them in ethical questions and discussions. The special interest group on IT & Society is always open and available to discuss personal as well as general aspects and questions related to IT ethics.

Links

ACM Updates Code of Ethics. Association of Computing Machinery, 2018-07-17

Ethische Leitlinien. Gesellschaft für Informatik, accessed 2018-09-16

In an Open Letter, Microsoft Employees Urge the Company To Not Bid on the US Military's Project JEDI. Slashdot, 2018-10-14

Tech Workers Now Want to Know: What Are We Building This For? The New York Times, 2018-10-07

Google Staff Tell Bosses China Censorship Is "Moral and Ethical" Crisis. The Intercept, 2018-08-16

Senior Google Scientist Resigns Over "Forfeiture of Our Values" in China. The Intercept, 2018-09-13

When should a tech company refuse to build tools for the government? The Guardian, 2018-06-26

Employees Of Another Major Tech Company Are Petitioning Government Contracts. Buzzfeed.News, 2018-06-26

Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts With Law Enforcement. Gizmodo, 2018-06-21

Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration. The New York Times, 2018-06-19

How a Pentagon Contract Became an Identity Crisis for Google. The New York Times, 2018-05-30

January 2019
SIG I&G

CODE OF ETHICS
Swiss Informatics Society SI

Präambel – Januar 2019

Die Fachgruppe “Informatik und Gesellschaft” der SI hat die Ethikrichtlinien der SI überarbeitet und wird sie der Generalversammlung 2019 zur Annahme vorlegen.

Warum braucht die SI Ethikrichtlinien? Auch wenn sie nicht immer so heissen, haben doch alle Berufsorganisationen Ethikrichtlinien. Diese Richtlinien helfen den Mitgliedern, sich in für die jeweilige Gruppe spezifischen ethischen Konfliktsituationen („richtig“) zu entscheiden. Ist es zum Beispiel für InformatikerInnen ethisch verantwortbar, an einem Projekt mitzuarbeiten, mit dessen Hilfe die Kriegsführung durch Drohnen optimiert wird? Fragen wie diese haben sich gerade in jüngster Zeit vielen unserer KollegInnen in USA gestellt (s. die Links am Ende des Textes).

Ethikrichtlinien sind kein unpersönlicher, binärer Algorithmus, in dem man eine ethische Fragestellung eingeben könnte, so dass alle Menschen die gleiche Antwort (Ja oder Nein) erhalten würden. Richtlinien formulieren allgemeine und fachlich/berufliche Werte, an denen sich InformatikerInnen orientieren können, um zu einer ethischen Entscheidung zu kommen. Dies bedeutet auch, dass in vielen Fällen unterschiedliche Personen auf Basis der Ethikrichtlinien zu unterschiedlichen Schlüssen kommen können.

Warum muss der SI-Ethikcode überarbeitet werden? Die bisher gültigen „alten“ Ethikrichtlinien wurden an der Generalversammlung 2005 verabschiedet, also z.B. noch vor der Erfindung des iPhone. Seit der letzten Aktualisierung hat die Informatik unsere Gesellschaft und Wirtschaft noch viel stärker durchdrungen, und die Arbeit von InformatikerInnen hat heute weit grössere Auswirkungen auf das Leben aller Menschen. Daraus folgt auch eine noch grössere Verantwortung von uns InformatikerInnen, die Digitalisierung möglichst gesellschaftsverträglich mitzugestalten, z.B. in dem wir unseren MitbürgerInnen nicht nur die Chancen, sondern auch die Risiken der Digitalisierung bewusst machen.

Insgesamt sind die neuen Ethikrichtlinien den alten sehr ähnlich. Änderungen gibt es vor allem dort, wo der Code Antworten und Hilfestellungen für den Umgang mit den disruptiven Aspekten der Digitalisierung bieten will (Künstliche Intelligenz, Datenschutz und Privacy).

Warum wurde der Ethikcode der ACM übernommen? Wir haben auch für den neuen Code den unserer US-amerikanischen Schwestergesellschaft, der ACM, übernommen. Zum einen sind wir fachlich/inhaltlich von ihm überzeugt, insbesondere weil er versucht, Fragestellungen aufgrund von neuen Entwicklungen (künstliche Intelligenz, soziale Netzwerke) aufzugreifen. Ausserdem ging der Aktualisierung des Codes innerhalb der ACM eine überaus intensive Diskussion voraus, von der wir nun profitieren können. Nicht zuletzt ist die Übernahme des Codes auch ein Ausdruck unserer Einbettung in das weltweite Netz von InformatikerInnen und Informatikgesellschaften.

Nicht geändert hat sich die Struktur der Ethikrichtlinien. Sie bestehen nach wie vor aus vier Teilen:

1. Allgemeine Prinzipien über die Rolle und Verantwortung der InformatikerInnen in der Gesellschaft;
2. Prinzipien bzgl. Informatik als Beruf;
3. Prinzipien für InformatikerInnen, die eine Vorbildfunktion haben, sei es als Vorgesetzte, Experte, Lehrer oder Ausbilder;
4. Die Durchsetzung des Codes.

Wir hoffen, dass die neuen Ethikrichtlinien gelebt werden und den SI-Mitgliedern Hilfe und Unterstützung in ethischen Fragen bieten. Die Fachgruppe „Informatik und Gesellschaft“ ist immer interessiert und bereit, persönliche wie auch allgemeine Fragen und Probleme der IT-Ethik zu diskutieren.

Links

ACM Updates Code of Ethics. Association of Computing Machinery, 2018-07-17

Ethische Leitlinien. Gesellschaft für Informatik, accessed 2018-09-16

In an Open Letter, Microsoft Employees Urge the Company To Not Bid on the US Military's Project JEDI. Slashdot, 2018-10-14

Tech Workers Now Want to Know: What Are We Building This For? The New York Times, 2018-10-07

Google Staff Tell Bosses China Censorship Is "Moral and Ethical" Crisis. The Intercept, 2018-08-16

Senior Google Scientist Resigns Over "Forfeiture of Our Values" in China. The Intercept, 2018-09-13

When should a tech company refuse to build tools for the government? The Guardian, 2018-06-26

Employees Of Another Major Tech Company Are Petitioning Government Contracts. Buzzfeed.News, 2018-06-26

Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts With Law Enforcement. Gizmodo, 2018-06-21

Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration. The New York Times, 2018-06-19

How a Pentagon Contract Became an Identity Crisis for Google. The New York Times, 2018-05-30

January 2019
SIG I&G