SQUIRE PATTON BOGGS

Ten Things About Artificial Intelligence (AI) for GCs in 2024

With AI, in all its forms, increasingly pervading our lives, as we utilize its abilities to assist our businesses in operating more effectively, it is essential to understand the global legal and regulatory framework that impacts its use. We provide 10 insights below as a guide of the issues. But, in short, our global team stands ready with expertise and specialized tools to help you successfully navigate these issues. Please do not hesitate to reach out to your contact at the firm, or one listed below with any query.

Here are some insights to help you assess your obligations and risks.

1. Ensure Your Legal Team and Key Stakeholders Are Educated on AI Risks and Regulation

While lawmakers consider specific AI laws, existing legal and regulatory schemes across the globe to regulate AI. Both need to be considered in developing an AI strategy and will need to be monitored as the law evolves to catch up with this disruptive technology. AI practices will need to undergo assessments to weigh benefits against risks, stakeholders need to be educated on the risks and management needs to evaluate risk tolerance and commercial prudence. This is not a "one and done" exercise. As the technology quickly evolves, risk profiles will shift, and legal paradigms will be developing. Ongoing stakeholder education and participation in policy making is essential.

2. Understand What Is and Not AI and the Related Terms of Art

At its core, AI is the automated processing of data, based on training data and processing prompts, that generates outputs such as predictions, recommendations or objectives. Different laws use different definitions, and a lot of other AI jargon is floating around. Being aware of key terms and making sure that your team is using common definitions when discussing AI risks and policy is key for risk management. The Federal Trade Commission (FTC) warns: "AI is defined in many ways and often in broad terms ... it may depend on who is defining it and for whom ... what matters more is output and impact." For this reason, we have included a lexicon as an appendix.

3. Apply Existing Laws and Regulations

Privacy and consumer protection laws and regulations, the regulators who enforce them and their scrutiny of AI are here to stay. The initial ban of ChatGPT by the Italian data protection authority and the investigations by a handful of others have made it clear that privacy and data protection should be at the top of mind for any companies implementing AI applications, particularly where personal data/personal information are implicated. AI hype is unlikely to die down anytime soon, including the attention from regulators. This is exacerbated if the inputs or outputs of the AI involve more than one jurisdiction. Privacy laws are territory specific, and many of these have cross-border transfer restrictions or requirements. Like the UK and EU, most of the new US state privacy laws address automated decision making and profiling, which are generally AI-driven. US state and federal consumer protection laws that govern deceptive and unfair acts and practices in commerce also apply beyond use of personal data, and anti-discrimination laws in jurisdictions worldwide may be implicated if protected categories of information are used as inputs or the output has a biased impact. In The Asia–Pacific (APAC) several jurisdictions have data localization rules that will make AI-related processing particularly tricky. While in certain countries, a simple transfer contract will suffice, others have adopted whitelists/adequacy determinations or even blacklists for data transfers to specific territories.

Human Resources (HR) AI applications are particularly risky due to existing employment, privacy and other laws. In Europe, even if candidates declare their express consent for the use of AI, an employee whose characteristics are used for matching, probably will be deemed to not have freely given consent. In addition, works councils may have "co-determination" rights with regard to the implementation of AI (especially if it may significantly change company processes or enable performance or behavior control. In many jurisdictions, these trigger the co-determination rights of works councils, trade unions or other employee representative committees. In particular, in Germany, a country with historically strong works council rights, most AI applications will require the prior signing of an agreement with the work council. Violating a works councils' co-determination rights may lead to criminal fines in some countries, including Germany.

California's omnibus privacy law now fully applies to California HR data as of January 1, 2023, and the California privacy agency has published draft regulations for discussion purposes on automated decision-making and profiling, including regarding employee monitoring and HR decision making, that will likely have a sweeping effect on the use of AI in HR matters.

New York City's law regulating the use of AI in employment decisions (Local Law 144) is in effect and enforcement took effect on July 5, 2023.

Intellectual property (IP) concerns and the overlap between AI and IP protection and enforcement are vast. Companies need to consider these issues when seeking IP protection (e.g., patents and copyrights) and when assessing the risk of IP infringement, such as through the input of third-party data, images, content and other IP materials into a Generative AI system, and the content generated by those systems. There have been dozens of lawsuits filed in the US alleging that LLMs and GAI infringe the copyrights of the owners of the content used to train the AI by using their IP without consent, as well as claims that some outputs include enough of the training content to constitute infringing derivative works. AI operators are claiming "fair use" as a defense, a doctrine that is complex and unevenly applied and is unavailable under the copyright laws of many other major market nations. Indeed, many key IP issues and concepts differ across jurisdictions, such as the liability for IP violations created by generative AI systems and whether its content is entitled to IP protection.

4. **AI Is Top of Mind for Lawmakers and Regulators Around the World – What follows is a brief global roundup of key developments:**

- **US**: AI-specific legislation is under consideration at the state and federal level. Meanwhile President Biden's executive order on AI has triggered a flurry of AI-related activity. Federal regulators and some attorney generals also are active in monitoring how AI is used. The FTC's Business Blog published no fewer than seven blog posts specifically about AI in 2023. Other federal agencies are also active as the CFPB, EEOC, SEC, Department of Health and Human Services have all taken action to regulate the use of AI to protect against discrimination, bias and other harms. AI regulation is showing up in the expanding state privacy law landscape, such as rules proposed in the California Consumer Privacy Act for AI risk assessments and election protection laws, such as Washington's law protecting against the use of realistic but purposefully false characteristics of a candidate.
- **Canada** is advancing comprehensive AI legislation – the Artificial Intelligence and Data Act – to regulate how AI is developed and used. .
- **UK**: the government does not plan to introduce specific new legislation or to create a new regulator to oversee AI. This reflects the UK government's concern that excessive or inappropriate regulation might stifle innovation. Instead, the UK government's proposals seek to allow existing regulators to take a tailored approach to the use of AI in their sectors by reference to six core principle which require developers and users to:
  - Ensure that AI is used safely;
  - Ensure that AI is technically secure and functions as designed;
  - Make sure that AI is appropriately transparent and explainable;
  - Consider fairness;
  - Identify a legal person to be responsible for AI;
  - Clarify routes to redress or contestability.

  Relevant initiatives involving existing regulators include the Financial Conduct Authority's "digital sandbox", allowing developers to collaborate and test innovations using GDPR-compliant datasets, the Competition and Markets Authority's report on the potential competition and consumer impact of foundation models and the Information Commissioner's best practice guidance for ensuring that AI complies with data protection laws.

  UK courts have also seen litigation concerning intellectual property rights in the context of AI. Ongoing cases include "input" claims that techniques such as webscraping to obtain data for use in AI training models infringe copyright and "output" claims that text or images generated by AI reproduce substantial parts of protected works and infringe intellectual property rights. The UK Supreme Court has also recently found that AI cannot be regarded as an "inventor" for the purposes of patent protection as the relevant legislation requires identification of a human inventor.
- **EU:** the supervisory bodies (among them, data protection ones) have not waited for specific AI legislation and looked at AI through the lens of data protection law, launching investigations into the use of personal data to train AI, and, in some territories, have even taken action (including temporary bans in Italy) on providers of AI services.
- **China** has issued various rules and standards relating to generative AI. The provision of generative AI services to the public is subject to several Internet service provision (or value-added telecom) licenses, some of which are restricted to foreign entities. Certain types of AI tools must pass government security assessments and the generative AI algorithm adopted by such tools has to be filed and registered with the government. The generative AI service provider is responsible for ensuring the legal compliance of the content, IP, safety and privacy rights. Content generated by AI must contain "marks" (such as watermarks) denoting it was generated by AI.
- **Japan** has issued an AI framework specifying concerns over the potential for the risk to individual privacy, IP infringement, public safety, use to spread disinformation and the utilization to commit crime. Although it has previously embraced the broad ingestion of copyrighted material to train AI models, it is currently re-thinking that position and recently issued a draft position attempting to balance the proper training of AI with concerns about the damage caused to content providers particularly through its output.
- **Hong Kong SAR**'s data protection regulator has published the Guidance on the Ethical Development and Use of Artificial Intelligence to help organizations understand and comply with the requirements under the Personal Data (Privacy) Ordinance (Cap. 486) when developing and using AI. The Hong Kong Monetary Authority has also published industry-specific guidance on the use of AI.
- **Singapore** has published a Model AI Governance Framework, and is consulting on a proposed one for generative AI specifically. ASEAN has a guide on governance and ethics for traditional (i.e. non-generative) AI.
- **South Korea**'s Science, ICT, and Broadcasting Committee of the Korean Assembly has passed its Act on Promotion of AI Industry and Framework for Establishing Trustworthy AI. There is an effort now to determine how it will specifically roll-out to providers.

Finally, private litigants are bringing cases alleging a variety of claims regarding inputs and outputs, as already noted above.

5. **Develop a Global AI Governance Policy and Framework** – A policy and a framework for applying the policy to AI development and use is crucial to ensuring legal compliance, ethical processing and risk minimization. Remember to think globally to the extent you operate across borders. To do so:

- Determine where you are positioned. Is your company an AI user, an AI provider or both? This informs the potential risks and impacts, and how to address them.
- Define what AI means in your organization and your use cases. Without a clear and common definition and an understanding of how your company is using AI, it will be impossible to build an AI framework. Certainly, definitions from applicable legal frameworks should be considered. See the appendix for a lexicon of terms.
- Leverage existing processes and procedures to address AI risks and impact: privacy and data governance, third-party risk/vendor assessments and so on.
- Involve necessary stakeholders (e.g., IT, InfoGov, Privacy, Security, Legal, HR, Marketing, etc.) into the process of developing and operating the company's policy and framework for development and implementation.
- Don't reinvent the wheel. Borrow and incorporate responsible AI Principles from existing frameworks, such as OECD, NIST, and ICO/IEC:
  - Ethical purpose
  - Accountability
  - Transparency
  - Fairness and non-discrimination
  - Respects privacy, confidentiality and proprietary rights
  - Complies with applicable laws
  - Safe, reliable and secure

6. **Conduct Risk and Impact Assessments** – Internal development of AI and the use of third-party AI tools should undergo an initial risk and ongoing impact assessments to identify risks of harm, the appropriateness of inputs, the credibility, non-bias and non-infringement of outputs and the effectiveness of mitigation efforts. This assessment should be conducted in whatever jurisdiction where you have implemented an AI solution in order to determine your obligations and risks. Numerous new and proposed laws and industry frameworks call for risk and impact assessments, including in relation to fundamental rights, and requirements vary by jurisdiction and can be expected to change over time. We are rolling out a new assessment toolkit, including an AI/ADM/Profiling module, to help you effectively consider current laws and best practices, which can be integrated into OneTrust and other data governance software platforms. In addition, claims you make about AI need to be assessed as any other marketing claim. In short, key components of assessments are:

- **Assess inputs** – AI is dependent upon training the AI with data sets to develop and improve the processing that powers AI. First, biased, stale and faulty inputs will result in output errors and other harms. Next, unauthorized use personal data and third-party intellectual property can result in claims related to both the use of the training data to train the AI, as well as arising out of the derivatives created from its processing. Finally, unless otherwise agreed with third party AI providers, such as in a license for a private instance of the AI tool, use of company confidential and proprietary data may be used for non-company use, threatening trade secrets and intellectual property protections (i.e., use licensed AI that protects your inputs, rather than free public versions that do not).
- **Assess outputs** – The outputs of AI system are essentially derivative works of the inputs, and if the inputs lacked sufficient consent to the use, the outputs could infringe third party personal and proprietary rights. Also, there may be issues regarding the ownership of the outputs. Does the AI provider contractually take or share ownership? In the US, works not established by human authorship are not entitled to copyright protection and thus, the company could, depending on the context, lack the exclusive rights or authorship that come with copyright if AI generates the content. A different conclusion has been reached in China, where the courts have found AI generated works to still be copyrightable with an entity, so long as there was a sufficient level of human creativity involved, such as from that entity's employee. Finally, outputs may lack credibility and accuracy (e.g., AI "hallucinations," which could be libelous or otherwise harmful due to inaccuracy) and absent proper controls, can be objectionable in a variety of ways (e.g., biased, profane or relating to illegal or undesirable activities). Note: licensed private instances of AI may allow for custom controls not available in free public versions.
- **Assess Decisions You Make Based on AI Output** – With many jurisdictions requiring that the result of any autonomous decision-making to be fair and unbiased, as well with the increasing prevalence of deep fakes, AI hallucinations or other disinformation, it is important to consider the decisions that will rely on AI output.
- **Ensure that claims you make about your use of AI and your AI-enabled products, are accurate, not misleading and substantiated.**

7.	**Contracting Related to the Use of AI Technology Is Particularly Thorny Because of the Newness of Most AI Technology and the Rapidly Evolving Legal Landscape** – Parties on both sides must carefully consider privacy, confidentiality, data protection, data ownership, use rights, as well as the more traditional terms related to warranties, indemnities, limitations and exclusions. For example, an AI technology provider usually offers its AI technology "As Is", reflecting the position that risk with technological innovations is a cost of doing business. On the other hand, the AI technology user's position is likely that the AI technology provider must stand behind its technology, such as providing risk and impact assessments, verifying that use of the technology will not harm any individual affected by its use. Further, the AI tech provider often asserts that data ingested by, and processed through, the technology may be utilized to improve the technology. However, the technology user often wants to ensure that the personal and confidential information that it submits to and through the AI technology, remains private and confidential. Many AI providers offer the ability to license a private instance for a fee that allows for greater protection for the licensor, including custom controls and confidentiality of inputs and outputs.
8.	**Consider Cybersecurity and Incident Response** – As part of the development and deployment of any AI system, IT security needs to consider how to secure any sensitive data that will be used in connection with the system, how to respond in the event of a security compromise and update its information security plan to address the AI system.
9.	**Consider Data Subject Rights** – If an AI system will process personal data, consider both the lawful basis for the use of the personal data, as well as how a data subject's right to request access, objection to processing and deletion/erasure can be honored as applicable across any jurisdictions where operated.
10.	**Treat AI Governance as a Business Imperative and Compliance Imperative** – • Business Imperative – ChatGPT has catalyzed the discussion around, and often adoption of, AI. This likely has your C-suite buzzing. AI governance will enable you to be a trusted advisor and solution provider not a roadblock to try to avoid. • Compliance Imperative – Effective AI governance will assist your organization in complying with existing laws and will be necessary to comply with existing and forthcoming AI-specific regulation such as the AI Act. If your company is an AI provider, in the next two to three years, there almost certainly will be laws requiring not only your organization's AI governance and compliance, but also your customers' compliance. If your company is an AI consumer, it will still face legal limitations, obligations and risks, including reputational risk if prudent decisions are not made to ensure that the benefits far outweigh the risk of harms.

Key Takeaways:

- Understand the context/use case involving AI:
  - Public, third party or internal use
  - End user interaction with AI? If so, who is the end user (employee, B2B customer, consumer, etc.)?
  - Developed internally or acquired from a third party
  - How are risk (before use) and impact (during use) being assessed, and by whom?
- Understand the inputs and outputs and how the processing works:
  - How are third party rights affected?
  - How are the company's rights affected?
- Understand what laws apply across the territories you are operating and ensure compliance.
- Determine what notices need to be provided to whom and when consents are required or prudent.
- Document assessments that establish that an AI system is used in a manner such that benefits outweigh potential harms.

How we can help – Our global team of experts and tools can help you identify and deal with these risks across the globe. The tools we offer include an initial high level stakeholder assessment survey, and grainular assessment templates and guidance for particular use cases, as well as model AI and InfoGov policies and educational materials. Please do not hesitate to reach out to your firm contact or one of the individuals listed below to explore how.

Appendix

The term "artificial intelligence" or "AI" has evolved as a catch-all term for a continuum of technology by which algorithms use inputs to produce outputs. On one end of the continuum is task-specific automated processing that can handle large amounts of data to complete a task infinitely faster than a human could complete the same task. On the other end is so-called artificial general intelligence (AGI), which aims to produce output that is indistinguishable from the human mind.

There are several levels of AGI, with some solutions reaching the early stages, but it remains unclear whether the highest level of AGI is achievable. Regardless, between the task-specific algorithms and highest levels of AGI are increasingly powerful AI systems trained to draw inferences from massive data sets in order to achieve particular outcomes. This acceleration in algorithmic sophistication – made possible by the decreased cost and increased power of cloud computing – may explain why experts have not yet settled on a consensus definition for AI.

Following are some commonly used terms that help explain this technology continuum.

What is	
AI Hallucination	"...[AI] models generate incorrect outputs but articulate them convincingly." – *OECD.AI Policy Observatory*
Algorithm	A clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result. – NIST
Algorithmic Discrimination	When automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, color, ethnicity, sex ... religion, age, national origin, disability, veteran status, genetic information or any other classification protected by law. Depending on the specific circumstances, such algorithmic discrimination may violate legal protections. – Blueprint for an AI Bill of Rights
Anonymization	A process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party – ISO/IEC 29100:2011(en)
Artificial Intelligence System	" ... means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate output such as predictions, recommendations or decisions influencing physical or virtual environments," reads the text, seen by EURACTIV ..." (March 3, 2023) "An AI system is a machine-based system that can influence the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (e.g. with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy." – OECD

What is	
Automated Decision-Making*	"[T]he process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data . . . [ADM] often involves profiling, but it does not have to." – UK Information Commissioner's Office
Deep Fake	". . . believable, realistic videos, pictures, audio and text of events which never happened" created using artificial intelligence/machine learning – US Department of Homeland Security
General Purpose AI	"AI system that is trained on broad data at scale, is designed for generality of output and can be adapted to a wide range of tasks." – European Parliament
Generative AI	". . . create[s] new content in response to prompts based on their training data." – OECD
	"[C]olloquial term] used to refer to chatbots developed from large language models and to technology that simulates human activity, such as software that creates deepfake videos and voice clones." – US Federal Trade Commission
Large Language Models (LLMs)	A class of generative AI tools, such as ChatGPT, Bard and Minerva, trained on vast amounts of data, often with little concern for the accuracy of the information or personal or proprietary rights to it, to enable content development and problem solving upon request using natural language or to write a response as a human would, with great speed. However, inherent with the nature of the training data the output can be incorrect or biased, sometimes referred to as AI hallucinations. Also, LLMs that lack good controls can be used in inappropriate ways and generate output that is undesirable, such as counsel on illegal activities and objectional or bigoted responses. Private instances of LLMs can add additional company mandated controls beyond what the developers have programmed for public versions.
Machine Learning	". . . process using algorithms rather than procedural coding that enables learning from existing data in order to predict future outcomes." – ISO/IEC 35505 Part 1: Application of ISO/IEC 38500 to the governance of data
	"[A] branch of computational statistics that focuses on designing algorithms that can automatically and iteratively build analytical models from new data without explicitly programming the solution." – US-EU Trade and Technology Council Inaugural Joint Statement
OECD	Organisation for Economic Cooperation and Development
Profiling	"[A]ny form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." – General Data Protection Regulation, Art. 4(4)*
	''Profiling' means any form of automated processing of personal information, as further defined by regulations [yet to be promulgated], to evaluate certain personal aspects relating to a natural person and, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." – California Consumer Privacy Act as amended by the California Privacy Rights Act
Training Dataset	"'A training dataset is used to teach [AI] models to yield the desired output and includes inputs and outputs that are correctly categorized or 'labeled, which allow the [AI] model to learn over time." – US General Services Administration

For more information on AI and how to develop and implement an ethical AI policy and framework for your business, contact the authors:

APAC

Charmian Aw (Singapore)
E charmian.aw@squirepb.com

Lindsay Zhu (China)
E lindsay.zhu@squirepb.com

Nick Chan (Hong Kong)
E nick.chan@squirepb.com

Scott Warren (Japan/China)
E scott.warren@squirepb.com

EMEA

David Naylor (London)
E david.naylor@squirepb.com

Charles Helleputte (Brussels, Paris)
E charles.helleputte@squirepb.com

Dr. Annette Demmel (Berlin)
E annette.demmel@squirepb.com

Bartolomé Martín (Madrid)
E bartolome.martin@squirepb.com

United States

Alan L. Friel (Los Angeles)
E alan.friel@squirepb.com

Julia B. Jacobson (New York)
E julia.jacobson@squirepb.com

David Elkins (Palo Alto/San Francisco)
E david.elkins@squirepb.com

Kyle R. Fath (Los Angeles/New York)
E kyle.fath@squirepb.com

Glenn A. Brown (Atlanta)
E glenn.brown@squirepb.com

GDR
Ranked "Elite" by Global Data Review