This opinion is nonprecedential except as provided by
Minn. R. Civ. App. P. 136.01, subd. 1(c).

STATE OF MINNESOTA
IN COURT OF APPEALS
A22-0194

Brenda Lutzke,
Appellant,

vs.

Metropolitan Council, et al.,
Respondents.

Filed December 5, 2022
Affirmed
Jesson, Judge

Hennepin County District Court
File No. 27-CV-19-14453

Carl E. Christensen, Christopher Wilcox, Christensen Law Office PLLC, Minneapolis, Minnesota (for appellant)

Kate M. Baxter-Kauf, Rachel A. Kitze Collins, Brian D. Clark, Lockridge Grindal Nauen P.L.L.P., Minneapolis, Minnesota (for respondents)

Considered and decided by Gaïtas, Presiding Judge; Segal, Chief Judge; and Jesson, Judge.

NONPRECEDENTIAL OPINION

JESSON, Judge

Appellant Brenda Lutzke challenges the summary-judgment dismissal of her claims against respondents Metropolitan Council and its subsidiary Metro Transit (collectively the Metropolitan Council) for negligence and violation of the Minnesota Health Records Act, Minnesota Statutes sections 144.291-.298 (2020), arguing that the district court erred in

determining that the Metropolitan Council is entitled to immunity from the lawsuit and that there are genuine issues of material fact that prevent summary judgment. Because we conclude that the Metropolitan Council is entitled to statutory immunity, we affirm.

FACTS

On a Friday in May 2019, Tanisha Brown, an employee of the Metropolitan Council, took her work laptop and some physical files home for the weekend. The physical files included health-screening records and drug-and-alcohol test results for employees and job applicants. The Metropolitan Council retains both physical and digital copies of such records. After receiving the physical copies of the test results an employee, such as Brown, scans the results into digital form using the Metropolitan Council's document-management system. The employee should then transport the physical copies to an administration building in Minneapolis for storage. Consistent with this protocol Brown took her work laptop and the physical files home planning to work over the weekend and transfer the physical files to the storage building on Monday morning.

But on Sunday, Brown placed the files and laptop in the trunk of her vehicle intending to bring them with her to the laundromat to complete additional work while she did her laundry. She drove to the area of the laundromat but parked and went to a nearby thrift store prior to the laundromat. While inside the thrift store Brown looked outside and noticed that the trunk of her vehicle was open. She went outside and discovered that three tote bags had been stolen from her trunk. The bags contained the laptop, physical files, and various personal items. After checking to see if the thrift store had security cameras,

Brown called the police and then notified her supervisor of the theft. The stolen items were never recovered.

The stolen physical files potentially included health-screening or personal information regarding approximately 76 individuals, including Lutzke. Specifically, the Metropolitan Council's internal investigation determined that an employment-verification form regarding Lutzke may have been among the stolen files. The verification form existed because a month before the theft, Lutzke authorized the Metropolitan Council to release records of her employment, including the results of drug-and-alcohol testing,[1] to a third party with whom she was seeking employment as a bus driver. The form lists Lutzke's name, Social Security number, and contact information for the third-party employer and required information from the Metropolitan Council about accidents or positive drug-and-alcohol tests.

Shortly after receiving information regarding who was potentially impacted by the theft, the Metropolitan Council sent Lutzke a letter informing her that "paper copies of drug/alcohol testing data were stolen from an employee's vehicle" and "[t]he stolen data includes your name and Social Security Number." All the potentially affected individuals, including Lutzke, were given the opportunity to receive 12 months of credit-monitoring services at the Metropolitan Council's expense. Lutzke declined the offer. In addition to addressing the stolen paper files, the Metropolitan Council investigated what data may have

[1] Lutzke is employed as a bus driver with Metro Transit. As conditions of her employment, Lutzke was required to undergo an initial health screening that included drug-and-alcohol testing and to submit to random drug-and-alcohol tests after starting employment.

been accessed from the stolen laptop. The laptop was encrypted and password-protected, but if an individual were able to successfully log in to the laptop then the digital copies of the health-screening reports would be accessible through the data-management system. Information services remotely disabled the laptop the morning after the theft. An internal investigation did not reveal that any files had been accessed.

Lutzke commenced this action alleging violation of the Minnesota Health Records Act and negligence. Lutzke alleged that the Metropolitan Council violated the Minnesota Health Records Act because its agent released Lutzke's health records without her consent, and that the Metropolitan Council was negligent because it violated the duty of care owed to Lutzke by allowing her health records to be released without her consent. Lutzke later filed an amended complaint to add class allegations and moved for class certification of the claim under the health records act.

The Metropolitan Council moved for summary judgment on both claims. Following a motion hearing, the district court granted the motion for summary judgment and entered judgment accordingly. The district court determined that the Metropolitan Council was entitled to both statutory immunity and vicarious official immunity, and further concluded that Lutzke's Minnesota Health Records Act claim failed because she did not demonstrate that there was a release of her health records or that she suffered any damages. The district court then denied the motion for class certification as moot.

Lutzke appeals.

DECISION

On appeal from the grant of summary judgment, we review de novo whether there are any genuine issues of material fact and whether the district court erred in applying the law. *Ruiz v. 1st Fid. Loan Servicing, LLC*, 829 N.W.2d 53, 56 (Minn. 2013). "We view the evidence in the light most favorable to the party against whom summary judgment was granted." *STAR Ctrs., Inc. v. Faegre & Benson, L.L.P.*, 644 N.W.2d 72, 76-77 (Minn. 2002). A genuine issue of material fact exists and precludes summary judgment when there is "sufficient evidence to permit reasonable persons to draw different conclusions." *Schroeder v. St. Louis County*, 708 N.W.2d 497, 507 (Minn. 2006) (emphasis omitted).

Lutzke argues that the district court erred in determining that the Metropolitan Council is entitled to statutory immunity. The application of statutory immunity is a legal question that we review de novo. *Conlin v. City of St. Paul*, 605 N.W.2d 396, 400 (Minn. 2000).

We begin our de novo review with a backdrop on municipal liability. A municipality[2] is generally liable for torts "of its officers, employees and agents acting within the scope of their employment or duties." Minn. Stat. § 466.02 (2020). But statutory immunity is an exception to that general rule intended to prevent judicial review

[2] It is undisputed that the Metropolitan Council and Metro Transit meet the statutory definition of "municipality" for purposes of statutory immunity. *See* Minn. Stat. § 466.01, subd. 1 (2020) (defining "municipality" to include public corporations and political subdivisions).

of the policy-making decisions of executive and legislative bodies. *Minder v. Anoka County*, 677 N.W.2d 479, 483-84 (Minn. App. 2004).

Statutory immunity only protects municipalities from tort[3] liability for claims based upon the performance of a *discretionary* function or duty. Minn. Stat. § 466.03, subd. 6 (2020) (emphasis added). In determining whether conduct involves a discretionary function or duty, we distinguish between planning decisions and operational decisions. *Minder*, 677 N.W.2d at 484. Planning decisions involve matters of public policy and are considered discretionary actions, whereas operational decisions involve the day-to-day operation of the government and are not entitled to statutory immunity. *Id.* To obtain the protection of statutory immunity, a municipality must show that the alleged negligent conduct stems from a protected planning decision. *Conlin*, 605 N.W.2d at 402.

In order to determine whether the alleged negligence here is derived from a planning decision, we first "identify what governmental conduct is being challenged." *Minder*, 677 N.W.2d at 484. Lutzke's grievance stems from the theft of the laptop and physical files from Brown's vehicle, but her specific challenge is to the Metropolitan Council's "failure to implement procedures to effectuate the policy objectives related to the safekeeping of personal health information left in unattended vehicles." She argues that because the Metropolitan Council "did not have a specific policy related to the safekeeping of personal health information in paper and computer files when being transported in a

[3] Sovereign immunity from statutory claims is generally addressed under a different standard. Thus, even if we were to conclude that statutory immunity was unavailable, it would not necessarily follow that the state had waived immunity for claims under the health records act. Because the parties focus on statutory immunity, we also focus on that issue.

vehicle, and because they had no procedures implementing any general policy in any pertinent manner, they are not entitled to immunity." Put another way, Lutzke faults the Metropolitan Council's policies for not explicitly prohibiting Brown from leaving sensitive confidential information in the trunk of her car.

To address Lutzke's argument that the Metropolitan Council failed to have a specific policy regarding files being transported in a vehicle, we first examine the Metropolitan Council's policies on information security, password procedure, data practices, and the storage of physical files. We then turn to the issue of whether any gap in the policies is a planning decision, as opposed to an operations decision.

The Metropolitan Council's general policy on information security provides:

> Information and systems belonging to the Metropolitan Council *must be managed and protected so that confidentiality is maintained* (preventing information from unauthorized disclosure), *integrity is ensured* (preventing information and systems from accidental and malicious modification), and availability is guaranteed (ensuring the reliability and accessibility of data and resources to authorized individuals in a timely manner).
>
> . . . .
>
> The overall intention of this policy and its corresponding standards is to achieve and maintain an effective and appropriate level of information security within the Metropolitan Council and to reinforce the position of the Metropolitan Council as a trusted agency.
>
> All employees and agents of the Council must be aware of their responsibility with regard to the issue of security and be proactive in exercising this responsibility.

(Emphasis added.)

With respect to the work-issued laptop, the Metropolitan Council had in place a password-procedure policy. This policy sets requirements for passwords and states that the intention is "to establish a baseline for creation of strong passwords" to "reduce the risk of unauthorized access to servers, workstations and databases maintained by the Metropolitan Council." In addition to this policy, the laptop was also encrypted, programmed to lock after ten unsuccessful login attempts, and capable of being disabled remotely, which it was the morning after the theft.

The data-practices policy sets out the general procedure for responding to a data breach. Also, the Metropolitan Council had a procedure relating to the digitization and storage of physical files—specifically, the files were to be digitized and stored electronically using the data-management system and not saved on a hard drive, and then the physical files were taken to a storage building in case there was an issue with the digitized files.

Having reviewed the relevant security policies, we turn to the central question: was the failure to adopt a policy explicitly regarding the safe keeping of confidential information in unattended vehicles a planning decision protected by statutory immunity or an operational decision?

We conclude that the Metropolitan Council's determination in this regard solidly qualifies as a planning decision involving matters of policy. Here, the Metropolitan Council had policies in place regarding the storage of information, the protection of that data, and the response to data breaches. And while Lutzke argues that the password-procedure policy is not relevant, it is directly related to Lutzke's contention that

there were not adequate policies in place to safeguard private data stored on laptops. The password protection, encryption of the information, and ability to disable the laptop remotely were plainly designed to prevent the unauthorized access of the non-public data stored on the laptops. And the policies make clear that the need to safeguard non-public data and ensure the public's trust in the Metropolitan Council was a primary goal of the policies. The policies were also developed "to achieve and maintain an effective and appropriate level of information security." We further observe that the failure to protect that data can expose the Metropolitan Council to legal liability. In sum, the Metropolitan Council's policies here involve considerations of safety issues, financial burdens, and possible legal consequences and fall squarely within the category of decisions that should not be second-guessed by the courts. *Watson by Hanson v. Metro. Transit Comm'n*, 553 N.W.2d 406, 412 (Minn. 1996) (quotation omitted).

Still, Lutzke argues that "[t]here is simply no cognizable political, social, or economic basis for an employer to adopt a policy permitting its employees to leave physical files and employer issued laptops containing medical records and personally identifiable information in their personal vehicles unattended in public spaces." But as the district court observed in its careful opinion, "it is unrealistic to expect an internal municipal policy to cover every possible contingency." And the record makes clear that there was a need for flexibility relating to how physical files and laptops were transported and stored. Brown explained, and the Metropolitan Council confirmed, that she needed to access the files and laptop on the weekend because there were time restraints for responding to positive drug-and-alcohol tests. The Metropolitan Council also permitted employees to work from

home and public places, and the physical files ultimately needed to be transported to the administrative building in Minneapolis for storage. We agree with the district court that it would be unrealistic to require the Metropolitan Council to have a policy related to every contingency possible based on the demonstrated need for flexibility.

Nor does *S.W. v. Spring Lake Park Sch. Dist. No. 16*, support Lutzke's argument that the lack of a specific policy precludes the application of statutory immunity. 580 N.W.2d 19 (Minn. 1998). In *S.W.*, a student was sexually assaulted in a school locker room after an individual entered the school and was seen, but not confronted, by multiple employees of the school. *Id.* at 21-22. The school did not have any security policy in place regarding visitors to the school. *Id.* at 23. The supreme court rejected the school district's argument that "the act of not putting a security policy in place is a decision entitled to statutory immunity." *Id.* But this case is distinguishable from *S.W.* Here, the Metropolitan Council has general policies in place that broadly address information security and establish safeguards for protected data. Lutzke challenges the *parameters* of the Metropolitan Council's security policies, not a *total lack* of a policy addressing information security akin to the situation in *S.W.*

Finally, we note that Lutzke's assertion that "[t]he lower court's holding permits [the Metropolitan Council] to violate the requirements" of the Minnesota Government Data Practices Act (Data Practices Act), Minnesota Statute sections 13.01-.90 (2020), is without merit. The Data Practices Act provides that "[n]otwithstanding section 466.03, a responsible authority or government entity which violates any provision of this chapter is liable to a person . . . who suffers any damages as a result of the violation." Minn.

Stat. § 13.08, subd. 1. The Data Practices Act therefore provides that an entity is liable for violations of the statute notwithstanding the statute governing statutory immunity. Additionally, "[i]n the case of a willful violation, the government entity shall. . . be liable to exemplary damages of not less than $1,000, nor more than $15,000 for each violation." *Id.* And "[a] responsible authority or government entity which violates or proposes to violate this chapter may be enjoined by the district court." *Id.*, subd. 2. Thus, if the Metropolitan Council was to violate the Data Practices Act, the act establishes a number of remedies that an aggrieved person may pursue, including damages, additional damages for particularly egregious violations, and injunctive relief. *Id.*, subds. 1, 2. Statutory immunity would not preclude the pursuit of such remedies. And here Lutzke did not assert a claim for violation of the Data Practices Act.

On this record, we conclude that the Metropolitan Council is entitled to statutory immunity.[4] The district court therefore did not err in granting the Metropolitan Council's motion for summary judgment.

Affirmed.

[4] Because we conclude that the Metropolitan Council is entitled to statutory immunity, we need not address the argument that it is also entitled to summary judgment based on vicarious official immunity and because there are no genuine issues of material fact related to the claims.